

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-145475

(43)Date of publication of application : 20.05.2004

(51)Int.Cl.

G06F 15/00
 G06F 12/00
 G06F 17/60
 G06K 7/00
 G06K 7/10
 G06K 17/00
 G06K 19/07
 G09C 1/00
 H04L 9/32

(21)Application number : 2002-307471

(71)Applicant : PATENT ONE KK

(22)Date of filing : 22.10.2002

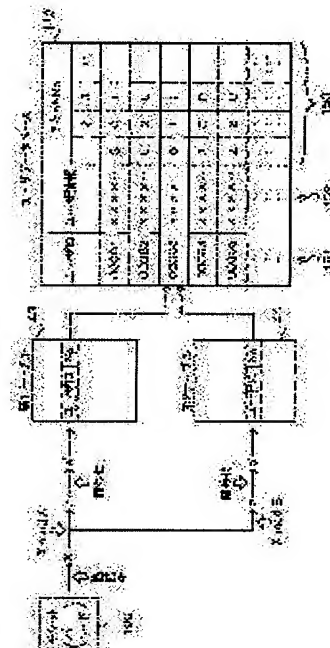
(72)Inventor : UGAWA TARO
 FURUMIZO SATOSHI

(54) IDENTIFICATION INFORMATION ISSUE SYSTEM AND METHOD, IDENTIFICATION INFORMATION AUTHENTICATION SYSTEM AND METHOD, AND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To accomplish both speed-up of an authentication process of identification information and improvement of security, and to allow each user to selectively use a plurality of pieces of identification information without increasing a processing amount.

SOLUTION: When an issue request including a user ID and a ticket No. is present, a ticket of a random pattern is generated and is digitalized. Residues (a), b are found by dividing the numerical value by divisors A, B, and an encrypted value a', b' are generated by encrypting the residues (a), b. When the same set is not registered in a storage position of the encrypted value a' of a first table 143 and a storage position of the encrypted value b' of a second table 144, the set of the user ID and the ticket No. included in the issue request is registered, and the ticket is transmitted to a request source. When the transmitted ticket is inputted, the encrypted values a', b' are similarly generated, and the ticket is authenticated when the same set is registered in the storage position of the encrypted value a' of the first table 143 and the storage position of the encrypted value b' of the second table 144.



(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-145475

(P2004-145475A)

(43) 公開日 平成16年5月20日(2004.5.20)

(51) Int. Cl.⁷

G06F 15/00
G06F 12/00
G06F 17/60
G06K 7/00
G06K 7/10

F I

G06F 15/00 330B
G06F 12/00 537A
G06F 17/60 140
G06F 17/60 512
G06K 7/00 U

テーマコード (参考)

5B035
5B058
5B072
5B082
5B085

審査請求 未請求 請求項の数 27 O L (全 34 頁) 最終頁に続く

(21) 出願番号 特願2002-307471 (P2002-307471)
(22) 出願日 平成14年10月22日 (2002.10.22)

(71) 出願人 501374714
パテントワン株式会社
東京都渋谷区渋谷3丁目17番4号
(74) 代理人 100104916
弁理士 古溝 聡
(72) 発明者 鶴川 太郎
東京都板橋区前野町2-33-15 エス
ポワール常盤台207号
(72) 発明者 古溝 聡
東京都北区十条仲原4-1-1 レールシ
ティ十条清水坂公園509号
Fターム(参考) 5B035 AA13 BB01 BB09 CA06
5B058 CA40 KA02 KA04 KA31 KA35
YA20
5B072 BB00 CC08 CC24 MM01 MM11
最終頁に続く

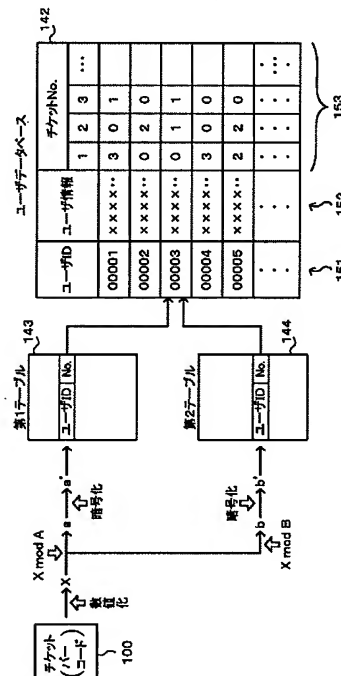
(54) 【発明の名称】 識別情報発行システム及び方法、識別情報認証システム及び方法、並びにプログラム

(57) 【要約】

【課題】 識別情報の認証処理の高速化とセキュリティの向上とを同時に達成すると共に、処理量を増大させることなく、各ユーザが複数の識別情報を使い分けられる。

【解決手段】 ユーザID及びチケットNo.を含む発行要求があると、ランダムなパターンのチケットを生成し、これを数値化する。この数値を除数A、Bで除算した剰余a、bを求め、これらをさらに暗号化した暗号化値a'、b'を生成する。第1テーブル143の暗号化値a'の記憶位置と第2テーブル144の暗号化値b'の記憶位置に、同一の組が登録されていなければ、発行要求に含まれるユーザID及びチケットNo.の組を登録し、チケットを要求元に送信する。送信したチケットが入力されると、同様にして暗号化値a'、b'が生成され、第1テーブル143の暗号化値a'の記憶位置と第2テーブル144の暗号化値b'の記憶位置に同一の組が登録されていれば、チケットを認証する。

【選択図】 図4



【特許請求の範囲】

【請求項 1】

1 人のユーザが複数の種別を使い分けられるようにした識別情報を発行する識別情報発行システムであって、
ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行要求を受信する発行要求受信手段と、
前記発行要求受信手段による発行要求の受信に応答して、識別情報を生成する識別情報生成手段と、
前記識別情報生成手段が生成した識別情報に基づいて、該生成した識別情報と 1 対 1 で対応付けられた数値組であって、複数の数値からなる数値組を生成する数値組生成手段と、
前記数値組に含まれる複数の数値にそれぞれ対応して用意された複数のテーブルと、
前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、ユーザを示す情報と識別情報の種別との組み合わせとして同一の組み合わせが登録されているかどうかを判別する登録判別手段と、
前記登録判別手段が同一の組み合わせが登録されていないと判別したときに、前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、前記発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録する組み合わせ登録手段と、
前記組み合わせ登録手段により各テーブルにユーザを示す情報と識別情報の種別とが組み合わせで登録された後に、前記識別情報生成手段が生成した識別情報を、前記発行要求したユーザに送信する識別情報送信手段と
を備えることを特徴とする識別情報発行システム。

10

20

【請求項 2】

前記識別情報送信手段により前記識別情報生成手段が生成した識別情報が送信された後、該識別情報を破棄する識別情報破棄手段をさらに備える
ことを特徴とする請求項 1 に記載の識別情報発行システム。

【請求項 3】

前記識別情報送信手段によりユーザに送信された識別情報に基づいて、前記数値組生成手段が数値組を生成するのと同様の方法により生成され、該送信された識別情報と 1 対 1 で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段と、
前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段と、
前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザに送信された識別情報を認証する認証手段とをさらに備える
ことを特徴とする請求項 1 または 2 に記載の識別情報発行システム。

30

【請求項 4】

前記識別情報送信手段がユーザに送信した識別情報を入力する識別情報入力手段を含むコンピュータ装置に接続され、
前記コンピュータ装置は、
前記識別情報入力手段から入力された識別情報に基づいて、前記数値組生成手段と同様の方法により、該入力された識別情報と 1 対 1 で対応付けられた数値組であって、複数の数値からなる数値組を生成する第 2 の数値組生成手段と、
前記第 2 の数値組生成手段が生成した数値組を前記識別情報発行システムに送信する数値組送信手段とを備え、
前記識別情報発行システムは、前記数値組送信手段から送信された数値組を受信する数値組受信手段をさらに備え、
前記組み合わせ抽出手段は、前記数値組受信手段が受信した数値組に含まれるそれぞれの

40

50

数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する

ことを特徴とする請求項 3 に記載の識別情報発行システム。

【請求項 5】

前記数値組生成手段は、

前記識別情報を所定の方法により数値化し、該識別情報と 1 対 1 で対応した数値を生成する数値生成手段と、

前記数値生成手段が生成した識別情報に対応した数値を、互いに異なる複数の除数で除算した剰余を算出し、各剰余を前記数値組に含まれる複数の数値とする剰余算出手段とを備え、

前記複数の除数の最小公倍数は、前記識別情報に対応した数値がとり得る値の最大値と最小値との差よりも大きい

ことを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の識別情報発行システム。

【請求項 6】

前記数値組生成手段は、

前記識別情報を所定の方法により数値化し、該識別情報と 1 対 1 で対応した数値を生成する数値生成手段と、

前記数値生成手段が生成した識別情報に対応した数値を、互いに異なる複数の除数で除算した剰余をそれぞれ算出する剰余算出手段と、

前記剰余算出手段が算出した各剰余を予め用意された暗号鍵を用いて暗号化した暗号化値を生成し、各暗号化値を前記数値組に含まれる複数の数値とする暗号化値生成手段とを備え、

前記複数の除数の最小公倍数は、前記識別情報に対応した数値がとり得る値の最大値と最小値との差よりも大きい

ことを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の識別情報発行システム。

【請求項 7】

前記各剰余を暗号化するための暗号鍵は、復号鍵とは非対称の暗号鍵である

ことを特徴とする請求項 6 に記載の識別情報発行システム。

【請求項 8】

前記数値生成手段が生成した数値を予め用意された暗号鍵を用いて暗号化する暗号化手段をさらに備え、

前記剰余算出手段は、前記暗号化手段が算出した剰余を前記複数の除数で除算した剰余をそれぞれ算出する

ことを特徴とする請求項 5 乃至 7 のいずれか 1 項に記載の識別情報発行システム。

【請求項 9】

前記数値を暗号化するための暗号鍵は、復号鍵とは非対称の暗号鍵である

ことを特徴とする請求項 8 に記載の識別情報発行システム。

【請求項 10】

ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報のキャンセル要求を受信するキャンセル要求受信手段と、

前記キャンセル要求をしたユーザを示す情報と発行要求された識別情報の種別との組み合わせを、前記複数のテーブルからそれぞれ削除する組み合わせ削除手段とをさらに備えることを特徴とする請求項 1 乃至 9 のいずれか 1 項に記載の識別情報発行システム。

【請求項 11】

ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の再発行要求を受信する再発行要求受信手段と、

前記再発行要求をしたユーザを示す情報と発行要求された識別情報の種別との組み合わせを、前記複数のテーブルからそれぞれ削除する組み合わせ削除手段と、

前記組み合わせ削除手段がユーザを示す情報と識別情報の種別との組み合わせを各テーブルから削除した後に、前記識別情報生成手段による識別情報の生成、前記数値組生成手段

10

20

30

40

50

による数値組の生成、前記登録判別手段による組み合わせの登録の判別、前記組み合わせ登録手段によるユーザを示す情報と識別情報の種別との組み合わせの登録、及び前記識別情報送信手段による識別情報の送信を、再度実行させる識別情報再発行手段とをさらに備える

ことを特徴とする請求項 1 乃至 10 のいずれか 1 項に記載の識別情報発行システム。

【請求項 12】

ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行予約を受信する発行予約受信手段と、

前記発行予約受信手段が受信した識別情報の発行予約を、該発行予約と共に受信したユーザを示す情報及び識別情報の種別に関連付けて登録する発行予約登録手段とをさらに備え

10

、
前記識別情報生成手段は、前記発行要求受信手段が識別情報の発行要求と共に受信したユーザを示す情報及び識別情報の種別に関連付けて、前記発行予約登録手段に発行予約が登録されているときに、識別情報を生成する

ことを特徴とする請求項 1 乃至 11 のいずれか 1 項に記載の識別情報発行システム。

【請求項 13】

前記発行要求受信手段は、ユーザが有する携帯端末装置から、該携帯端末装置固有の識別情報と共に、ユーザからの識別情報の発行要求を受信し、

前記識別情報発行システムは、前記識別情報生成手段が生成した識別情報を、前記発行要求受信手段が前記発行要求と共に受信した携帯端末装置固有の識別情報を暗号鍵として用いて暗号化する識別情報暗号化手段をさらに備え、

20

前記識別情報送信手段は、前記識別情報暗号化手段が暗号化した識別情報を前記発行要求を送信した携帯端末装置に送信し、

前記識別情報送信手段から送信された暗号化された識別情報は、該識別情報を受信した携帯端末装置において、該携帯端末装置固有の識別情報を復号鍵として復号化される

ことを特徴とする請求項 1 乃至 12 のいずれか 1 項に記載の識別情報発行システム。

【請求項 14】

前記識別情報は、一義的に特定可能な画像パターンによって構成される

ことを特徴とする請求項 1 乃至 13 のいずれか 1 項に記載の識別情報発行システム。

【請求項 15】

1 人のユーザが複数の種別を発行されて、使い分けられるようにした識別情報を認証する識別情報認証システムであって、

ユーザからの発行要求に応答して識別情報が生成されたときに、該識別情報と 1 対 1 で対応付けられた数値組に含まれる各数値に対応したそれぞれの記憶位置に、該識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録した複数のテーブルと、

識別情報が発行されたユーザから提示された識別情報に基づいて、前記テーブルへの登録時と同様の方法により生成され、該提示された識別情報と 1 対 1 で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段と、

40

前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段と、

前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザから提示された識別情報を認証する認証手段と

を備えることを特徴とする識別情報認証システム。

【請求項 16】

前記ユーザからの発行要求に応答して生成された識別情報は、前記複数のテーブルに識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録し、該ユーザに発行した後に破棄されている

50

ことを特徴とする請求項 15 に記載の識別情報認証システム。

【請求項 17】

前記識別情報は、一義的に特定可能な画像パターンによって構成されることを特徴とする請求項 15 または 16 に記載の識別情報認証システム。

【請求項 18】

1 人のユーザが複数の種別を使い分けられるようにした識別情報を発行する識別情報発行方法であって、

ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行要求を受信するステップと、

前記発行要求の受信に応答して、識別情報を生成するステップと、

10

前記生成した識別情報に基づいて、該生成した識別情報と 1 対 1 で対応付けられた数値組であって、複数の数値からなる数値組を生成するステップと、

前記数値組に含まれる複数の数値にそれぞれ対応する複数のテーブルを予め準備するステップと、

前記生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、ユーザを示す情報と識別情報の種別との組み合わせとして同一の組み合わせが登録されているかどうかを判別するステップと、

同一の組み合わせが登録されていないと判別したときに、前記生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、前記発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録するステップと、

20

各テーブルにユーザを示す情報と識別情報の種別とが組み合わせで登録された後に、前記生成した識別情報を発行要求をしたユーザに送信するステップと

を含むことを特徴とする識別情報発行方法。

【請求項 19】

前記生成した識別情報が送信された後、該識別情報を破棄するステップをさらに含むことを特徴とする請求項 18 に記載の識別情報発行方法。

【請求項 20】

前記ユーザに送信された識別情報に基づいて、前記生成された識別情報に基づいて数値組を生成するのと同様の方法により生成され、該送信された識別情報と 1 対 1 で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されて

30

いるユーザを示す情報と識別情報の種別との組み合わせを抽出するステップと、ユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定するステップと、

全てのテーブルから同一の組み合わせが抽出されたと判定したときに、前記ユーザに送信された識別情報を認証するステップとをさらに含む

ことを特徴とする請求項 18 または 19 に記載の識別情報発行方法。

【請求項 21】

1 人のユーザが複数の種別を発行されて、使い分けられるようにした識別情報を認証する識別情報認証方法であって、

ユーザからの発行要求に応答して識別情報が生成されたときに、該識別情報と 1 対 1 で対応付けられた数値組に含まれる各数値に対応したそれぞれの記憶位置に、該識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録する複数のテーブルを予め準備するステップと、

40

識別情報を発行されたユーザから提示された識別情報に基づいて、前記テーブルへの登録時と同様の方法により生成され、該提示された識別情報と 1 対 1 で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出するステップと、

ユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定するステップと、

全てのテーブルから同一の組み合わせが抽出されたと判定したときに、前記ユーザから提

50

示された識別情報を認証するステップと
を含むことを特徴とする識別情報認証方法。

【請求項 2 2】

前記ユーザからの発行要求に応答して生成された識別情報は、前記複数のテーブルに識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録し、該ユーザに発行した後に破棄されていることを特徴とする請求項 2 1 に記載の識別情報認証方法。

【請求項 2 3】

1 人のユーザが複数の種別を使い分けられるようにした識別情報を発行するためのプログラムであって、
ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行要求を受信する発行要求受信手段、
前記発行要求受信手段による発行要求の受信に応答して、識別情報を生成する識別情報生成手段、
前記識別情報生成手段が生成した識別情報に基づいて、該生成した識別情報と 1 対 1 で対応付けられた数値組であって、複数の数値からなる数値組を生成する数値組生成手段、
前記数値組に含まれる複数の数値にそれぞれ対応する複数のテーブルを予め準備するテーブル準備手段、
前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、ユーザを示す情報と識別情報の種別との組み合わせとして同一の組み合わせが登録されているかどうかを判別する登録判別手段、
前記登録判別手段が同一の組み合わせが登録されていないと判別したときに、前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、前記発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録する組み合わせ登録手段、及び、
前記組み合わせ登録手段により各テーブルにユーザを示す情報と識別情報の種別とが組み合わせで登録された後に、前記識別情報生成手段が生成した識別情報を発行要求をしたユーザに送信する識別情報送信手段
としてコンピュータ装置を機能させるためのプログラム。

【請求項 2 4】

前記識別情報送信手段により前記識別情報生成手段が生成した識別情報が送信された後、該識別情報を破棄する識別情報破棄手段
として前記コンピュータ装置をさらに機能させることを特徴とする請求項 2 3 に記載のプログラム。

【請求項 2 5】

前記識別情報送信手段によりユーザに送信された識別情報に基づいて、前記数値組生成手段が数値組を生成するのと同様の方法により生成され、該送信された識別情報と 1 対 1 で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段、
前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段、及び、
前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザに送信された識別情報を認証する認証手段
として前記コンピュータ装置をさらに機能させることを特徴とする請求項 2 3 または 2 4 に記載のプログラム。

【請求項 2 6】

1 人のユーザが複数の種別を発行されて、使い分けられるようにした識別情報を認証するためのプログラムであって、

ユーザからの発行要求に応答して識別情報が生成されたときに、該識別情報と1対1で対応付けられた数値組に含まれる各数値に対応したそれぞれの記憶位置に、該識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録する複数のテーブルを準備するテーブル準備手段、

識別情報を発行されたユーザから提示された識別情報に基づいて、前記テーブルへの登録時と同様の方法により生成され、該提示された識別情報と1対1で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段、

前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段、及び

前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザから提示された識別情報を認証する認証手段

としてコンピュータ装置を機能させるためのプログラム。

【請求項27】

前記ユーザからの発行要求に応答して生成された識別情報は、前記複数のテーブルに識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録し、該ユーザに発行した後に破棄されている

ことを特徴とする請求項26に記載のプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、イベントのチケットなどとして用いられる識別情報の発行及び認証に関するものである。

【0002】

【従来の技術】

近年、携帯電話技術は、急速に進歩しており、Web接続機能を有するものが一般的となり、また、表示装置の解像度も高くなっている。このような携帯電話技術の進歩に伴って、コンサートなどのイベントのチケットを携帯電話機上に表示されるバーコードによって構成し、Web接続サービスを利用して配信するものが登場している。

【0003】

携帯電話機に配信されたバーコードは、イベント会場の入口に設置されたコンピュータ装置が有するバーコードリーダによって読み取られ、これを発行した（管理する）サーバ装置に送られるものとなる。サーバ装置は、送られてきたバーコードが正当であるかどうかを認証し、正当なものであると認証できれば、その旨を入口のコンピュータ装置に通知するものとなる。この通知に従って、チケットとしてのバーコードを購入したユーザが、イベント会場に入場することが認められる。

【0004】

従来では、サーバ装置は、バーコードを発行して携帯電話機に配信すると共に、そのバーコードを内部のデータベースに保存するものとしていた。携帯電話機に表示されたバーコードがバーコードリーダによって読み取られて送られてくると、サーバ装置は、送られてきたバーコードを保存しておいたバーコードと照合することによって、そのバーコードが正当なものであることを認証するものとしていた（例えば、特許文献1参照）。

【0005】

【特許文献1】

特許第3207192号公報

【0006】

【発明が解決しようとする課題】

しかしながら、特許文献1の技術では、ユーザに発行された認証情報としてのバーコードは、少なくともそのバーコードを用いて認証を行うことが不要となるまで、サーバ装置内

10

20

30

40

50

に継続的に置かれることとなる。すると、サーバ装置がハッキングされることによって、認証情報であるバーコードが漏洩するという危険が非常に大きかった。

【0007】

認証情報としてのバーコードの漏洩は、サーバ装置内においてバーコードを暗号化して保存しておくことによって防止を図ることができる。しかし、バーコードを暗号化して保存しておくことにより、認証を行う際に暗号化したバーコードの復号化が必要となり、認証に要する処理が増大してしまう。

【0008】

暗号強度を低くすれば、認証に要する処理の増大は抑えられるが、暗号の解読によってバーコードが漏洩する危険は高くなる。逆に暗号強度を高くすれば、暗号の解読が困難であるためバーコードが漏洩する危険は低く抑えられるが、認証の際におけるバーコードの復号化が非常に複雑なものとなり、認証に要する処理量が大きくなってしまう。このように、特許文献1の技術では、認証処理の高速化とセキュリティの向上とを同時に達成することができなかった。

【0009】

ところで、コンサートなどのイベント、特に人気が高く、キャパシティが大きい会場でのイベントとなると、その開場時間から開始時間までの短い時間（例えば、1時間程度）において、数万人程度の人々がイベント会場に入場しようとする。イベントのチケットとして携帯電話機に表示されたバーコードを使用した場合、膨大な数のバーコードの認証処理を短時間の間で行わなければならない。

【0010】

十分なセキュリティを確保すべくサーバ装置内のバーコードを暗号化していた場合には、イベントの開場時間から開始時間までの短い時間での処理量が非常に大きなものとなる。入場時の混乱を避けるためには、サーバ装置のダウンは絶対に避けなければならないので、非常に処理能力が大きいサーバ装置を用意しておかななければならない。一方、開場時間より前や、開始時間よりも後になると、サーバ装置において行われる処理はあまりない。すると、短期的にサーバ装置の稼働率が高くなることはあっても、平均の稼働率は低いものにとどまっており、サーバ装置の処理能力を十分に生かし切れない。

【0011】

また、特許文献1では、1人のユーザが認証情報として使用するバーコードは1つだけであることを前提としているが、コンサートなどのイベントのチケットとしてバーコードを使用する場合には、1人のユーザに複数のバーコードを使用させる必要がある。1人のユーザが複数のバーコードを使用する場合、認証の際にバーコードの照合を行わなければならない回数、ユーザの数ではなく、最大でバーコードの数だけ、平均でもバーコードの数の半分となる。すると、1人のユーザが使用できるバーコードの数が多くなればなるほど、処理量も増大してしまうという問題があった。

【0012】

本発明は、識別情報の発行及び認証において、認証処理の高速化とセキュリティの向上とを同時に達成することができる識別情報発行システム等を提供することを目的とする。

【0013】

本発明は、また、識別情報の発行及び認証において、1人のユーザが複数の識別情報を使い分けても、処理量をあまり増大させることがない識別情報発行システム等を提供することを目的とする。

【0014】

【課題を解決するための手段】

上記目的を達成するため、本発明の第1の観点にかかる識別情報発行システムは、1人のユーザが複数の種別を使い分けられるようにした識別情報を発行する識別情報発行システムであって、ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行要求を受信する発行要求受信手段と、

10

20

30

40

50

前記発行要求受信手段による発行要求の受信に応答して、識別情報を生成する識別情報生成手段と、

前記識別情報生成手段が生成した識別情報に基づいて、該生成した識別情報と1対1で対応付けられた数値組であって、複数の数値からなる数値組を生成する数値組生成手段と、

前記数値組に含まれる複数の数値にそれぞれ対応して用意された複数のテーブルと、

前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、ユーザを示す情報と識別情報の種別との組み合わせとして同一の組み合わせが登録されているかどうかを判別する登録判別手段と、

前記登録判別手段が同一の組み合わせが登録されていないと判別したときに、前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、前記発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録する組み合わせ登録手段と、

前記組み合わせ登録手段により各テーブルにユーザを示す情報と識別情報の種別とが組み合わせで登録された後に、前記識別情報生成手段が生成した識別情報を、前記発行要求したユーザに送信する識別情報送信手段と

を備えることを特徴とする。

【0015】

上記識別情報発行システムは、

前記識別情報送信手段により前記識別情報生成手段が生成した識別情報が送信された後、該識別情報を破棄する識別情報破棄手段をさらに備えるものとすることができる。

【0016】

上記識別情報発行システムでは、識別情報生成手段が生成した識別情報に基づいて数値組が求められ、数値組に含まれる複数の数値に対応した各テーブルの記憶位置にユーザを示す情報と識別情報の種別とが組み合わせで登録される。このように識別情報に応じて記憶位置を定めて各テーブルへの登録を行うことにより、後述するように識別情報の認証を行う際に、識別情報同士を照合する必要がなくなる。このため、識別情報生成手段が生成した識別情報が識別情報送信手段によりユーザに送信された後は、上記識別情報発行システム内に識別情報そのものを残しておく必要がなく、識別情報破棄手段によって破棄してしまってもよい。

【0017】

上記識別情報発行システムは、内部に識別情報そのものが残っていないので、仮にハッカーに侵入されても各ユーザの識別情報が盗み出されることがなく、高度のセキュリティを達成することができる。また、テーブルのための記憶容量は必要となるが、識別情報そのもののための記憶容量は必要ないので、特に識別情報の情報量が大きいときには、システムに必要な記憶容量も小さくすることができる。さらに、テーブルには、ユーザを示す情報と識別情報の種別とを組み合わせで登録するため、後述するように1人のユーザが複数の識別情報を使い分ける場合において、識別情報の種別までを認証できるようになる。

【0018】

なお、数値組生成手段が数値組を生成するために用いる識別情報と、識別情報送信手段がユーザに送信する識別情報とは、完全に一致したものとは限らない。例えば、識別情報生成手段は、まず特定の数値を生成し、この数値から数値組生成手段が数値組を生成するものとし、識別情報送信手段は、前記特定の数値から双方向で一義的に定められる特定の情報を送信するものとしてもよい。前記特定の数値と前記特定の情報とは、ここでは、実質的な内容としては同じ識別情報であると見ることができる。

【0019】

上記識別情報発行システムは、

前記識別情報送信手段によりユーザに送信された識別情報に基づいて、前記数値組生成手段が数値組を生成するのと同様の方法により生成され、該送信された識別情報と1対1で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ

10

20

30

40

50

抽出手段と、

前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段と、

前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザに送信された識別情報を認証する認証手段とをさらに備えるものとすることができる。

【0020】

このような構成を備えることにより、組み合わせ抽出手段が各テーブルからユーザを示す情報と識別情報の種別との組み合わせを抽出し、組み合わせ判定手段が同一の組み合わせが抽出されたかどうかを判定すれば、識別情報の認証を行える。各テーブルには識別情報の種別まで登録されているので、ユーザだけでなく種別の認証も行える。

10

【0021】

ここで行う認証の処理は、各テーブルに登録されているユーザを示す情報と識別情報の種別の抽出と、その比較だけでよいので、識別情報同士を照合する場合に比べて高速な処理が行える。識別情報の照合ではないので、システム内部に残した識別情報の復号化といった処理量を増大させる処理も必要ない。しかも、発行した識別情報の数が増加しても、処理量の増加はそれよりもずっと少ない。従って、1人のユーザが複数の種別の識別情報を使い分けるものとしても、認証処理の処理量があまり増大しない。

【0022】

この場合において、上記識別情報発行システムは、

20

前記識別情報送信手段がユーザに送信した識別情報を入力する識別情報入力手段を含むコンピュータ装置に接続されていてもよい。ここで、

前記コンピュータ装置は、

前記識別情報入力手段から入力された識別情報に基づいて、前記数値組生成手段と同様の方法により、該入力された識別情報と1対1で対応付けられた数値組であって、複数の数値からなる数値組を生成する第2の数値組生成手段と、

前記第2の数値組生成手段が生成した数値組を前記識別情報発行システムに送信する数値組送信手段とを備えるものとすることができ、

前記識別情報発行システムは、前記数値組送信手段から送信された数値組を受信する数値組受信手段をさらに備えるものとすることができる。そして、

30

前記組み合わせ抽出手段は、前記数値組受信手段が受信した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出するものとすることができる。

【0023】

この場合、ユーザに送信された識別情報に基づいて数値組を生成するまでの処理は、別のコンピュータ装置において行うものとなっている。例えば、識別情報がイベントのチケットなどとして用いられる場合には、短時間の間に処理が集中するが、識別情報の入力から数値組の生成という比較的処理量が大きくなる処理は、分散して行うことができる。

【0024】

上記識別情報発行システムにおいて、

40

前記数値組生成手段は、例えば、

前記識別情報を所定の方法により数値化し、該識別情報と1対1で対応した数値を生成する数値生成手段と、

前記数値生成手段が生成した識別情報に対応した数値を、互いに異なる複数の除数で除算した剰余を算出し、各剰余を前記数値組に含まれる複数の数値とする剰余算出手段とを備えるものとすることができる。ここで、

前記複数の除数の最小公倍数は、前記識別情報に対応した数値がとり得る値の最大値と最小値との差よりも大きいことが条件となる。

【0025】

前記数値組生成手段は、また、

50

前記識別情報を所定の方法により数値化し、該識別情報と1対1で対応した数値を生成する数値生成手段と、

前記数値生成手段が生成した識別情報に対応した数値を、互いに異なる複数の除数で除算した剰余をそれぞれ算出する剰余算出手段と、

前記剰余算出手段が算出した各剰余を予め用意された暗号鍵を用いて暗号化した暗号化値を生成し、各暗号化値を前記数値組に含まれる複数の数値とする暗号化値生成手段とを備えるものとすることができる。ここでも、

前記複数の除数の最小公倍数は、前記識別情報に対応した数値がとり得る値の最大値と最小値との差よりも大きいことが条件となる。

【0026】

なお、前記各剰余を暗号化するための暗号鍵は、復号鍵とは非対称の暗号鍵であることが好ましい。

【0027】

さらに、前記数値組生成手段を上記の2通りのいずれかで構成した場合、上記識別情報発行システムは、

前記数値生成手段が生成した数値を予め用意された暗号鍵を用いて暗号化する暗号化手段をさらに備えるものとすることができ、

前記剰余算出手段は、前記暗号化手段が算出した剰余を前記複数の除数で除算した剰余をそれぞれ算出するものとすることができる。

【0028】

なお、前記数値を暗号化するための暗号鍵も、復号鍵とは非対称の暗号鍵であることが好ましい。

【0029】

上記のように識別情報生成手段が生成した識別情報から数値組を生成すると、異なる識別情報から生成された数値組では、数値組に含まれる全ての数値が一致することはなくなる。これにより、数値組から識別情報を一義的に定めることができる。識別情報に対応した数値から求めた各剰余を暗号化した暗号化値を、各テーブルへの記憶位置として適用することで、上記識別情報発行システムからテーブルの情報を盗み出し、これを解析しても剰余の値が分からないので、元の識別情報を復元できない。特に暗号鍵として非対称鍵を適用すると、どこにも復号鍵がないので情報を盗み出して復号を行うことができず、元の識別情報の復元は、どのような暗号技術に比べても遜色がないか、それ以上に困難なものとなる。

【0030】

上記識別情報発行システムは、

ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報のキャンセル要求を受信するキャンセル要求受信手段と、

前記キャンセル要求をしたユーザを示す情報と発行要求された識別情報の種別との組み合わせを、前記複数のテーブルからそれぞれ削除する組み合わせ削除手段とをさらに備えるものとすることができる。

【0031】

上記識別情報発行システムは、

ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の再発行要求を受信する再発行要求受信手段と、

前記再発行要求をしたユーザを示す情報と発行要求された識別情報の種別との組み合わせを、前記複数のテーブルからそれぞれ削除する組み合わせ削除手段と、

前記組み合わせ削除手段がユーザを示す情報と識別情報の種別との組み合わせを各テーブルから削除した後に、前記識別情報生成手段による識別情報の生成、前記数値組生成手段による数値組の生成、前記登録判別手段による組み合わせの登録の判別、前記組み合わせ登録手段によるユーザを示す情報と識別情報の種別との組み合わせの登録、及び前記識別情報送信手段による識別情報の送信を、再度実行させる識別情報再発行手段とをさらに備

10

20

30

40

50

えるものとすることもできる。

【0032】

このような構成を備えるものとすることで、上記識別情報発行システムの内部に発行済みの識別情報が残っていても、ユーザは、識別情報のキャンセルや再発行を受けることができるようになる。ところで、識別情報のキャンセルや再発行を行う場合、比較的处理量が多い各テーブルのサーチが必要となっている。識別情報がイベントのチケットなどとして用いられる場合であっても、キャンセルや再発行の要求が短時間に集中することはほとんどあり得ないので、処理量として特に問題になることはない。

【0033】

上記識別情報発行システムは、

ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行予約を受信する発行予約受信手段と、

前記発行予約受信手段が受信した識別情報の発行予約を、該発行予約と共に受信したユーザを示す情報及び識別情報の種別に関連付けて登録する発行予約登録手段とをさらに備えるものとすることができる。この場合において、

前記識別情報生成手段は、前記発行要求受信手段が識別情報の発行要求と共に受信したユーザを示す情報及び識別情報の種別に関連付けて、前記発行予約登録手段に発行予約が登録されているときに、識別情報を生成することができる。

【0034】

識別情報がイベントのチケットなどとして用いられる場合は、申し込み受付を開始してから短時間の間で多くの申し込みがある場合がある。申し込みが集中する時間には、上記したような発行予約登録だけを行うものとするれば、この発行予約登録の処理量は比較的小さいので、上記識別情報発行システムに、必要以上に大きな処理負荷がかかることはない。そして、比較的处理量の大きい識別情報の実際の発行は、発行予約を登録した後に処理を分散して行うことができるようになる。

【0035】

上記識別情報発行システムにおいて、

前記発行要求受信手段は、ユーザが有する携帯端末装置から、該携帯端末装置固有の識別情報と共に、ユーザからの識別情報の発行要求を受信するものであってもよい。この場合において、

前記識別情報発行システムは、前記識別情報生成手段が生成した識別情報を、前記発行要求受信手段が前記発行要求と共に受信した携帯端末装置固有の識別情報を暗号鍵として用いて暗号化する識別情報暗号化手段をさらに備えるものとすることができ、

前記識別情報送信手段は、前記識別情報暗号化手段が暗号化した識別情報を前記発行要求を送信した携帯端末装置に送信するものとすることができる。この場合において、

前記識別情報送信手段から送信された暗号化された識別情報は、該識別情報を受信した携帯端末装置において、該携帯端末装置固有の識別情報を復号鍵として復号化されるものとするればよい。

【0036】

この場合、識別情報の発行要求をした携帯端末装置以外では、識別情報が正しく復号されない。このため、識別情報送信手段から送信して携帯端末装置に届くまでの間で識別情報が盗み出されたり、不正な転送があったとしても、正当に識別情報の発行を受けた者以外は、正しい識別情報を得ることができない。これにより、識別情報の不正使用を防ぐことができる。

【0037】

上記識別情報発行システムにおいて、

前記識別情報は、一義的に特定可能な画像パターンによって構成されるものとすることができる。

【0038】

識別情報を画像パターンによって構成するものとした場合、従来では、これを記憶してお

10

20

30

40

50

くのにかなりの記憶容量が必要となった。また、照合の処理量が大きなものとなっていた。特に複雑な画像パターンを適用したときには、これらの問題が大きくなる。これに対して、上記識別情報発行システムでは、識別情報のための記憶容量や照合の処理が全く必要ないので、識別情報として複雑な画像パターンを適用しても、記憶容量の増大や処理量の増大の問題を発生させることがない。

【0039】

上記目的を達成するため、本発明の第2の観点にかかる識別情報認証システムは、1人のユーザが複数の種別を発行されて、使い分けられるようにした識別情報を認証する識別情報認証システムであって、

ユーザからの発行要求に応答して識別情報が生成されたときに、該識別情報と1対1で対応付けられた数値組に含まれる各数値に対応したそれぞれの記憶位置に、該識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録した複数のテーブルと、

識別情報を発行されたユーザから提示された識別情報に基づいて、前記テーブルへの登録時と同様の方法により生成され、該提示された識別情報と1対1で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段と、

前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段と、

前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザから提示された識別情報を認証する認証手段と

を備えることを特徴とする。

【0040】

上記識別情報認証システムにおいて、

前記ユーザからの発行要求に応答して生成された識別情報は、前記複数のテーブルに識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録し、該ユーザに発行した後に破棄されていてもよい。

【0041】

上記識別情報認証システムでは、組み合わせ抽出手段が各テーブルからユーザを示す情報と識別情報の種別との組み合わせを抽出し、組み合わせ判定手段が同一の組み合わせが抽出されたかどうかを判定すれば、識別情報の認証を行える。各テーブルには識別情報の種別まで登録されているので、ユーザだけでなく種別の認証も行える。

【0042】

ここで行う認証の処理は、各テーブルに登録されているユーザを示す情報と識別情報の種別の抽出と、その比較だけでよいので、識別情報同士を照合する場合に比べて高速な処理が行える。識別情報の照合ではないので、システム内部に残した識別情報の復号化といった処理量を増大させる処理も必要ない。しかも、発行した識別情報の数が増加しても、処理量の増加はそれよりもずっと少ない。従って、1人のユーザが複数の種別の識別情報を使い分けるものとしても、認証処理の処理量があまり増大しない。

【0043】

さらに、識別情報同士の照合によって認証を行うのではないので、識別情報そのものを、上記識別情報認証システム内に残しておく必要がなく、各テーブルへの登録が終了し、識別情報をユーザに発行した後には破棄されている。このように内部に識別情報そのものが残っていないので、仮にハッカーに侵入されても各ユーザの識別情報が盗み出されることがなく、高度のセキュリティを達成することができる。また、テーブルのための記憶容量は必要となるが、識別情報そのもののための記憶容量は必要ないので、特に識別情報の情報量が大きいときには、システムに必要な記憶容量も小さくすることができる。

【0044】

上記識別情報認証システムにおいて、

前記識別情報は、一義的に特定可能な画像パターンによって構成されるものとすることができる。

【0045】

識別情報を画像パターンによって構成するものとした場合、従来では、これを記憶しておくのにかなりの記憶容量が必要となった。また、照合の処理量が大きなものとなっていた。特に複雑な画像パターンを適用したときには、これらの問題が大きくなる。これに対して、上記識別情報認証システムでは、識別情報のための記憶容量や照合の処理が全く必要ないので、識別情報として複雑な画像パターンを適用しても、記憶容量の増大や処理量の増大の問題を発生させることがない。

【0046】

上記目的を達成するため、本発明の第3の観点にかかる識別情報発行方法は、1人のユーザが複数の種別を使い分けられるようにした識別情報を発行する識別情報発行方法であって、

ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行要求を受信するステップと、

前記発行要求の受信に応答して、識別情報を生成するステップと、

前記生成した識別情報に基づいて、該生成した識別情報と1対1で対応付けられた数値組であって、複数の数値からなる数値組を生成するステップと、

前記数値組に含まれる複数の数値にそれぞれ対応する複数のテーブルを予め準備するステップと、

前記生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、ユーザを示す情報と識別情報の種別との組み合わせとして同一の組み合わせが登録されているかどうかを判別するステップと、

同一の組み合わせが登録されていないと判別したときに、前記生成した数値組に含まれるそれぞれの数値に対応した各テーブルに記憶位置に、前記発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録するステップと、

各テーブルにユーザを示す情報と識別情報の種別とが組み合わせで登録された後に、前記生成した識別情報を発行要求をしたユーザに送信するステップとを含むことを特徴とする。

【0047】

上記識別情報発行方法は、

前記生成した識別情報が送信された後、該識別情報を破棄するステップをさらに含むものとしてもよい。

【0048】

上記識別情報発行方法は、

前記ユーザに送信された識別情報に基づいて、前記生成された識別情報に基づいて数値組を生成するのと同様の方法により生成され、該送信された識別情報と1対1で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出するステップと、

ユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定するステップと、

全てのテーブルから同一の組み合わせが抽出されたと判定したときに、前記ユーザに送信された識別情報を認証するステップとをさらに含むものとしてもよい。

【0049】

上記目的を達成するため、本発明の第4の観点にかかる識別情報認証方法は、1人のユーザが複数の種別を発行されて、使い分けられるようにした識別情報を認証する識別情報認証方法であって、

ユーザからの発行要求に応答して識別情報が生成されたときに、該識別情報と1対1で対応付けられた数値組に含まれる各数値に対応したそれぞれの記憶位置に、該識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録す

10

20

30

40

50

る複数のテーブルを予め準備するステップと、
識別情報を発行されたユーザから提示された識別情報に基づいて、前記テーブルへの登録時と同様の方法により生成され、該提示された識別情報と1対1で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出するステップと、
ユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定するステップと、
全てのテーブルから同一の組み合わせが抽出されたと判定したときに、前記ユーザから提示された識別情報を認証するステップと
を含むことを特徴とする。

10

【0050】

上記識別情報発行方法において、
前記ユーザからの発行要求に応答して生成された識別情報は、前記複数のテーブルに識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録し、該ユーザに発行した後に破棄されていてもよい。

【0051】

上記目的を達成するため、本発明の第5の観点にかかるプログラムは、
1人のユーザが複数の種別を使い分けられるようにした識別情報を発行するためのプログラムであって、
ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行要求を受信する発行要求受信手段、
前記発行要求受信手段による発行要求を受信に応答して、識別情報を生成する識別情報生成手段、
前記識別情報生成手段が生成した識別情報に基づいて、該生成した識別情報と1対1で対応付けられた数値組であって、複数の数値からなる数値組を生成する数値組生成手段、
前記数値組に含まれる複数の数値にそれぞれ対応する複数のテーブルを予め準備するテーブル準備手段、
前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、ユーザを示す情報と識別情報の種別との組み合わせとして同一の組み合わせが登録されているかどうかを判別する登録判別手段、
前記登録判別手段が同一の組み合わせが登録されていないと判別したときに、前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、前記発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録する組み合わせ登録手段、及び、
前記組み合わせ登録手段により各テーブルにユーザを示す情報と識別情報の種別とが組み合わせで登録された後に、前記識別情報生成手段が生成した識別情報を発行要求をしたユーザに送信する識別情報送信手段
としてコンピュータ装置を機能させることを特徴とする。

20

30

【0052】

上記第5の観点にかかるプログラムは、
前記識別情報送信手段により前記識別情報生成手段が生成した識別情報が送信された後、該識別情報を破棄する識別情報破棄手段
として前記コンピュータ装置をさらに機能させるものであってもよい。

40

【0053】

上記第5の観点にかかるプログラムは、
前記識別情報送信手段によりユーザに送信された識別情報に基づいて、前記数値組生成手段が数値組を生成するのと同様の方法により生成され、該送信された識別情報と1対1で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段、

50

前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段、及び、

前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザに送信された識別情報を認証する認証手段

として前記コンピュータ装置をさらに機能させるものであってもよい。

【0054】

上記目的を達成するため、本発明の第6の観点にかかるプログラムは、

1人のユーザが複数の種別を発行されて、使い分けられるようにした識別情報を認証するためのプログラムであって、

ユーザからの発行要求に応答して識別情報が生成されたときに、該識別情報と1対1で対応付けられた数値組に含まれる各数値に対応したそれぞれの記憶位置に、該識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録する複数のテーブルを準備するテーブル準備手段、

識別情報を発行されたユーザから提示された識別情報に基づいて、前記テーブルへの登録時と同様の方法により生成され、該提示された識別情報と1対1で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段、

前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段、及び

前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザから提示された識別情報を認証する認証手段

としてコンピュータ装置を機能させることを特徴とする。

【0055】

上記第6の観点にかかるプログラムにおいて、

前記ユーザからの発行要求に応答して生成された識別情報は、前記複数のテーブルに識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせで登録し、該ユーザに発行した後に破棄されていてもよい。

【0056】

【発明の実施の形態】

以下、添付図面を参照して、本発明の実施の形態について説明する。

【0057】

図1は、この実施の形態にかかるチケット発行システムを示すブロック図である。このチケット発行システムは、予め登録したユーザがコンサートやスポーツなどのイベントのチケットを購入し、購入したチケットの認証を受けて、イベント会場に入場できるようにしたものである。チケットが認証されるということは、そのチケットが当該イベントについてのチケットであるということを確認するということである。なお、このチケット発行システムで発行するチケットとしては、二次元バーコードが用いられている。

【0058】

図示するように、このチケット発行システムは、サーバ装置1と、入場ゲート装置2と、登録したユーザが管理する携帯電話機3とを含んでいる。サーバ装置1及び入場ゲート装置2は、チケット発行者が管理するものであり、両者間は、専用線4で接続されている。携帯電話機3は、Web接続機能を備えるものであり、携帯電話網6からインターネット5に入り、サーバ装置1に接続できるようになっている。

【0059】

サーバ装置1は、チケットの発行及び認証を管理するコンピュータ装置である。入場ゲート装置2は、イベント会場の入口に設置されるもので、イベント会場内への人の出入りを規制するものである。入場ゲート装置2は、図では1つだけ示しているが、実際にはイベント会場の入口に複数設置される。携帯電話機3は、サーバ装置1が発行したチケットを

10

20

30

40

50

受信し、表示するものである。次に、サーバ装置 1、入場ゲート装置 2、及び携帯電話機 3 の詳細について説明するものとする。

【0060】

図 2 は、図 1 のサーバ装置 1 の構成を示すブロック図である。図示するように、サーバ装置 1 は、CPU (Central Processing Unit) 11 と、主記憶装置 12 と、通信装置 13 と、補助記憶装置 14 とを備えている。補助記憶装置 14 には、プログラムファイル 141、ユーザデータベース 142、第 1 テーブル 143 及び第 2 テーブル 144 が記憶されている。

【0061】

CPU 11 は、主記憶装置 12 に転送されたプログラムを実行し、後述するように、チケットの予約、販売、キャンセル、再発行、認証などの種々の処理を行う。チケットの構成については後述する。主記憶装置 12 は、CPU 11 の主記憶領域を提供するもので、プログラムファイル 141 のプログラムが転送され、また、CPU 11 の作業領域として用いられる。通信装置 13 は、専用線 4 を介して入場ゲート装置 2 と情報を送受信すると共に、インターネット 5 及び携帯電話網 6 を介して携帯電話機 3 と情報を送受信する。

【0062】

補助記憶装置 14 は、CPU 11 の補助記憶領域を提供するもので、固定ディスク装置などによって構成される。プログラムファイル 141 は、後述するフローチャートに示すプログラムを含むファイルである。ユーザデータベース 142 は、このチケット発行システムを利用してチケットを購入し、そのチケットによる認証を受けて、イベント会場に入場できるユーザに関する情報を登録したデータベースである。第 1 テーブル 143 及び第 2 テーブル 144 は、個々のチケットとユーザ及びチケットの種別とを対応付けるために用いられるテーブルである。ユーザデータベース 142、第 1 テーブル 143 及び第 2 テーブル 144 の詳細については後述する。

【0063】

図 3 は、このチケット発行システムにおいて適用されるチケットの例を示す図である。図では、携帯電話機 3 の表示装置に表示された状態を示している。図示するように、このチケット 100 は、二階調の二次元バーコードによって構成されており、その四隅には方向チェックマーク 101～104 が設けられている。方向チェックマーク 101～104 は、チケットの方向を示すもので、1 つだけ明表示されるチェックマーク 104 がチケットの右下であることを示している。

【0064】

チェックマーク 101～104 以外のチケット表示部 105 については、チケット No. とは無関係に、そのパターンを任意に選ぶことができるが、選ばれたパターンは、曖昧性がなく一義的に特定される。もっとも、チケット表示部 105 に特定の情報を含ませるため、一部の特定の場所が特定のパターンを有するものとなっても構わない。チケット 100 の二次元バーコードとしてのパターンは、所定の方法により数値化することができ、パターンと数値とは 1 対 1 で対応する。なお、チケット 100 のパターンを数値化するプログラムは、サーバ装置 1 と入場ゲート装置 2 内に格納されているだけで、外部には公開されていない。

【0065】

図 4 は、ユーザデータベース 142、第 1 テーブル 143 及び第 2 テーブル 144 の詳細を示す図である。図示するように、ユーザデータベース 142 は、登録したユーザ毎に、ユーザ ID 151、ユーザ情報 152、複数のチケット情報 153 を登録したデータベースとなっている。ユーザ ID 151 は、各ユーザを一意に識別するための情報であり、チケットの予約や購入などの際には、このユーザ ID が必要となる。

【0066】

ユーザ情報 152 は、各ユーザの属性に関する情報を含む。ユーザの属性に関する情報としては、少なくともユーザが設定した（或いはユーザ登録の際に通知された）パスワードと、チケット 100 の二次元バーコードを画像データとして携帯電話機 3 に送信するため

10

20

30

40

50

のアドレスを含んでいる。その他、ユーザ情報 152 としては、従来のシステムで適用されてきたような種々の情報を含むものとするができる。

【0067】

チケット情報 153 には、イベントの種別（開始日時によっても異なる）毎に固有のチケット No. に対応して、ユーザのチケットの予約、購入、使用状況を示すフラグが登録されている。フラグの値が 0 であれば未予約を、1 であれば予約済みであるが未購入を、2 であれば購入済みであるが未使用（イベント会場に入場していないこと）を、3 であれば使用済み（イベント会場に入場したこと）を示している。

【0068】

第 1 テーブル 143 及び第 2 テーブル 144 には、ユーザが何らかのイベントのチケット 100 を購入したときに、そのユーザのユーザ ID 151 と購入したチケットのチケット No. との組が、チケット 100 のパターンに応じた記憶位置において記憶される。第 1 テーブル 143 及び第 2 テーブル 144 からは、ユーザ ID をキーとしてユーザデータベース 142 を参照することができる。

【0069】

次に、ユーザ ID 及びチケット No. の組が、第 1 テーブル 143 及び第 2 テーブル 144 の記憶位置のどこに記憶されるかについて説明する。二次元バーコードからなるチケット 100 が発行されると、そのパターンに 1 対 1 で対応した整数値となるように数値化される。チケット 100 が数値化された数値 X は、第 1 テーブル 143 に対応した除数 A（整数値）と、第 2 テーブル 144 に対応した除数 B（整数値）とで除算され、それぞれの

10

20

【0070】

ここで、除数 A と除数 B との最小公倍数は、数値 X がとりうる最大値 X_{max} と最小値 X_{min} の差よりも大きいという関係がある。また、除数 A と除数 B とは、互いに素であることが好ましい。この条件を満たす限り、数値 X が異なれば、剰余 a と剰余 b との両方が一致するということはあり得ない。つまり、異なる数値 X に対しては、剰余 a と剰余 b の組み合わせが全て異なっており、剰余 a と剰余 b の組み合わせは、チケット 100 のパターンと 1 対 1 で対応するものとなっている。

30

【0071】

剰余 a と剰余 b とが求められると、それぞれ所定の暗号鍵を用いて暗号化され、暗号化値 a' 、 b' が生成される。この暗号鍵は、復号鍵が異なる非対称暗号系の暗号鍵である。また、剰余 a を暗号化する暗号鍵と剰余 b を暗号化する暗号鍵とは、異なるものであることが好ましい。剰余 a と剰余 b の組み合わせは、チケット 100 のパターンと 1 対 1 で対応するので、暗号化値 a' と暗号化値 b' の組み合わせも、チケット 100 のパターンと 1 対 1 で対応するものとなる。

40

【0072】

発行されたチケット 100 についてユーザ ID 及びチケット No. の組は、第 1 テーブル 143 の暗号化値 a' に対応した記憶位置と、第 2 テーブル 144 の暗号化値 b' に対応した記憶位置とに登録されるものとなる。異なるチケット 100 であっても、剰余 a、b のいずれか一方が一致することあるので、同様に暗号化値 a' 、 b' のいずれか一方が一致することはある。暗号化値 a' 、 b' のいずれか一方が一致していても、ユーザ ID 及びチケット No. の組は、第 1 テーブル 143 及び第 2 テーブル 144 のいずれか一方において、同じ記憶位置へ重複して登録される（実際には、リストで繋ぐなどの処理が必要となる）。

【0073】

新たにチケット 100 を発行しようとする場合において生成したパターンが、そのチケット 100 から求めた暗号化値 a' に対応する第 1 テーブル 143 の記憶位置から取り出したユーザ ID 及びチケット No. の組と、暗号化値 b' に対応する第 2 テーブル 144 の記憶位置から取り出したユーザ ID 及びチケット No. の組とが一致すれば、そのチケット 100 は発行済みのものであることが分かる。この場合は、別のパターンが生成される

50

【0074】

また、ユーザが購入したチケット100を使ってイベント会場に入場しようとするときは、後述するように入場ゲート装置2においてユーザが購入したチケット100（携帯電話機3に表示された二次元バーコード）が読み取られるが、読み取られたチケット100からも同様に暗号化値a'と暗号化値b'とが求められる。

【0075】

求めた暗号化値a'に対応する第1テーブル143の記憶位置から取り出したユーザID及びチケットNo.の組と、暗号化値b'に対応する第2テーブル144の記憶位置から取り出したユーザID及びチケットNo.の組を比較する。両者が一致して、かつチケットNo.が該当するイベントのものを示すときには、チケット100が正当なものと認証され、ユーザがイベント会場に入場できるようになる。

【0076】

図5は、図1の携帯電話機3の構成を示すブロック図である。図示するように、携帯電話機3は、CPU31と、ROM(Read Only Memory)32と、RAM(Random Access Memory)33と、入力装置34と、表示装置35と、通信装置36とを備えている。携帯電話機3は、このほかにも通話を行うために必要な構成要素を備えているが、本発明とは直接関係がないため、図5において省略している。

【0077】

CPU31は、ROM32に記憶されたプログラムを実行し、サーバ装置1から受信したチケットを管理する処理を行う。CPU31は、入力装置34からの入力に従って、チケット（二次元バーコード）を表示装置35に表示させる。ROM32は、CPU31の処理プログラムを記憶する。また、携帯電話機3の個体番号が格納されている。RAM33は、データの記憶領域として用いられるものであり、当該データの中には、チケットの画像データも含まれる。

【0078】

入力装置34は、「1」～「0」までの数字キー、「*」キー、「#」キーなどを含み、利用者の操作によって必要な情報をCPU31に入力する。表示装置35は、液晶表示装置などによって構成され、チケット（二次元バーコード）の画像を含む種々の情報を表示する。通信装置36は、インターネット5及び携帯電話網6を介してサーバ装置1と情報を送受信する。

【0079】

図6は、図1の入場ゲート装置2の構成を示すブロック図である。図示するように、入場ゲート装置2は、CPU21と、記憶装置（主記憶装置及び補助記憶装置を含む）22と、通信装置23と、バーコードリーダ24と、入場ゲート25と、アラーム装置26とを備えている。

【0080】

CPU21は、記憶装置22に記憶されたプログラムを実行し、携帯電話機3から読み取ったチケットに従ってサーバ装置1から送られてくる通知に従って、ゲートを開放させる、またはアラームを発報させるなどの処理を行う。記憶装置22は、CPU21の処理プログラムを記憶すると共に、データの記憶領域として用いられる。通信装置23は、インターネット5を介してサーバ装置1と情報を送受信する。

【0081】

バーコードリーダ24は、携帯電話機3の表示装置35に表示されたチケット（二次元バーコード）の画像を読み取る。入場ゲート25は、イベント会場の外側から内側に向けて一方向で開放するように構成されており、サーバ装置1から送られてくる通知に従って開放状態となり、ユーザが通過できるようになる。アラーム装置26は、サーバ装置1から送られてくる通知に従って、不正なチケットがあった旨のアラームを発報する。

【0082】

なお、サーバ装置1のプログラムファイル141に置かれているプログラム、入場ゲート

10

20

30

40

50

装置 2 の記憶装置に記憶されているプログラムは、いずれもオブジェクトコードで記述されたものであって、ソースコードで記述されたプログラムがサーバ装置 1 及び入場ゲート装置 2 には置かれていない。

【0083】

以下、この実施の形態にかかるチケット発行システムにおける処理について説明する。この実施の形態にかかるチケット発行システムを利用して、二次元バーコードからなるチケットを購入しようとする者は、予めユーザ登録を行って、ユーザデータベース 142 に登録しておく必要がある。もっとも、ユーザ登録の方法は、従来の方法と変わらないので、ここではユーザ登録が予めなされているものとし、以下の処理説明におけるユーザとは、ユーザ登録をしたユーザのことである。

10

【0084】

新たなイベントについてチケットの販売を行う場合、その予約受付を行うまでに当該チケットについてチケット No. が付与され、ユーザデータベース 142 にフラグ領域が設定され、その全てに 0 が設定されることとなる。新たなイベントについてチケットの販売を行う場合は、メールなどによってチケット No. と共に販売開始がユーザに告知される。なお、チケットの購入に伴う課金やキャンセルに伴う返金なども行われるが、これらの処理は本発明と関係がないので説明を省略する。

【0085】

ユーザは、チケットを購入する前段階として、ユーザはチケットの購入予約を行う。購入予約ができたユーザは、その予約に基づいてチケットの発行を受け、これを購入する。チケットを購入した後に、ユーザがそれをキャンセルする場合や、チケットをなくして再発行を受ける場合もある。そして、イベント会場の開場時間となると、ユーザが購入したチケットの認証を受け、イベント会場へと入場することとなる。

20

【0086】

つまり、この実施の形態にかかるチケット発行システムで行われる処理は、

- (1) チケット予約処理
- (2) チケット購入処理
- (3) チケットキャンセル処理
- (4) チケット再発行処理
- (5) チケット認証処理

30

の 5 つに大きく分けられることとなる。以下、それぞれについて詳しく説明する。

【0087】

図 7 は、チケット予約処理を示すフローチャートである。チケットを購入予約しようとするユーザは、まず、自己の携帯電話機 3 の入力装置 34 から、ユーザ ID とパスワードとを入力する。また、購入予約しようとするチケットのチケット No. を入力装置 34 から入力する (ステップ S101)。さらにユーザが入力装置 34 から購入予約の要求を入力すると、ステップ S101 で入力されたユーザ ID、パスワード及びチケット No. と共に予約要求が通信装置 36 からサーバ装置 1 に送信される (ステップ S102)。その後、CPU 31 は、サーバ装置 1 からの情報の受信待ちとなる。

【0088】

サーバ装置 1 では、通信装置 13 が携帯電話機 3 から送られてきた予約要求を受信する (ステップ S151)。この予約要求を受信すると、CPU 11 は、受信した予約要求に含まれるユーザ ID がユーザデータベース 142 に登録されているかどうかを判定する。さらに、パスワードが正しいかどうかを判定する (ステップ S152)。

40

【0089】

ユーザ ID が登録されていて、パスワードも正しい場合は、CPU 11 は、受信した予約要求に含まれるチケット No. のチケットが予約受付可能であるかどうか、すなわち予約受付を開始したチケットであって、売り切れとなっていないチケットであるかどうかを判定する (ステップ S153)。予約受付可能であれば、CPU 11 は、当該予約要求に含まれるユーザ ID 及びチケット No. に対応するユーザデータベース 142 のフラグを未

50

予約を示す0から予約済みを示す1に更新する（ステップS154）。

【0090】

フラグの更新が終了すると、CPU11は、予約要求をした携帯電話機3に宛てたメールで、通信装置13から予約完了通知を送信させる（ステップS155）。また、予約要求に含まれるユーザIDが登録されていないかパスワードが間違っていた場合、或いは予約要求に含まれるチケットNo.のチケットが予約受付不可であった場合には、CPU11は、予約要求をした携帯電話機3に宛てたメールで、通信装置13から予約不可通知を送信させる（ステップS156）。予約完了通知または予約不可通知の送信により、サーバ装置1の側における処理は終了となる。

【0091】

携帯電話機3では、通信装置36がステップS155で送信された予約完了通知またはステップS156で送信された予約不可通知を受信する（ステップS103）。CPU31は、受信した予約完了通知または予約不可通知を表示装置35に表示させて、ユーザに示す（ステップS104）。これで、チケット予約処理が終了する。

【0092】

図8は、チケット購入処理を示すフローチャートである。チケット購入処理においても、ユーザは、自己の携帯電話機3の入力装置34から、ユーザIDとパスワードとを入力する。また、予約したチケットのうちから購入しようとするチケットのチケットNo.を入力装置34から入力する（ステップS201）。さらにユーザが入力装置から購入の要求を入力すると、ステップS201で入力されたユーザID、パスワード及びチケットNo.と共に購入要求が通信装置36からサーバ装置1に送信される（ステップS202）。その後、CPU31は、サーバ装置1からの情報の受信待ちとなる。

【0093】

サーバ装置1では、通信装置13が携帯電話機3から送られてきた購入要求を受信する（ステップS251）。この購入要求を受信すると、CPU11は、受信した購入要求に含まれるユーザIDがユーザデータベース142に登録されているかどうかを判定する。さらに、パスワードが正しいかどうかを判定する（ステップS252）。

【0094】

ユーザIDが登録されていて、パスワードも正しい場合には、CPU11は、受信した購入要求に含まれるユーザID及びチケットNo.に対応するユーザデータベース142のフラグの状態がチケットの予約済みを示す1になっているかどうかを判定する（ステップS253）。

【0095】

フラグの状態がチケットの予約済みを示す1になっていれば、CPU11は、ランダムにパターンを決定して二次元バーコードからなるチケット100を生成する（ステップS254）。CPU11は、生成したチケットが既に発行済みのチケット（後述するように使用不能とされたものを含まない）のパターンと同じであるかどうかをチェックする発行済みチケットチェック処理を行う（ステップS255）。

【0096】

図9（a）は、ステップS255の発行済みチケットチェック処理を詳細に示すフローチャートである。発行済みチケット生成処理では、CPU11は、ステップS254で生成したチケットのパターンに対応した数値Xを生成する（ステップS301）。さらに、CPU11は、チケットを数値化した数値Xを除数Aで除算して剰余aを求め、また、数値Xを除数Bで除算して剰余bを求める（ステップS302）。

【0097】

CPU11は、求めた剰余aを所定の暗号鍵を用いて暗号化して暗号化値a'を生成し、また、剰余bも同様に暗号化して暗号化値b'を生成する（ステップS303）。暗号化値a'、b'が生成されると、CPU11は、暗号化値a'、b'を用いて第1テーブル143及び第2テーブル144をそれぞれ参照することにより、ステップS301で数値化したチケットが発行済みのものであるかどうかをチェックするテーブルチェック処理を、

10

20

30

40

50

行う（ステップS304）。

【0098】

図9（b）は、ステップS304のテーブルチェック処理を詳細に示すフローチャートである。テーブルチェック処理では、CPU11は、第1テーブル143の暗号化値a'に対応する記憶位置に登録されているユーザID及びチケットNo.の組を取り出す（ステップS311）。また、第2テーブル144の暗号化値b'に対応する記憶位置に登録されているユーザID及びチケットNo.の組を取り出す（ステップS312）。

【0099】

CPU11は、こうして第1テーブル143及び第2テーブル144からユーザID及びチケットNo.の組を取り出すと、両者を比較し、ユーザIDとチケットNo.のいずれもが一致するかどうかを判定する（ステップS313）。一致していれば、CPU11は、一致を示す情報を返却して（ステップS314）、テーブルチェック処理を終了し、発行済みチケットチェック処理に復帰する。一致していなければ、CPU11は、不一致を示す情報を返却して（ステップS315）、テーブルチェック処理を終了し、発行済みチケットチェック処理に復帰する。

【0100】

図9（a）の発行済みチケットチェック処理に復帰すると、CPU11は、テーブルチェック処理から返却された情報が一致を示す情報か不一致を示す情報であるかを判定する（ステップS305）。不一致を示す情報であったならば、ステップS303で生成した暗号化値a'、b'と共にチケットが未発行を示す情報を返却して（ステップS306）、発行済みチケットチェック処理を終了し、図8のチケット購入処理に復帰する。一致を示す情報であったならば、発行済みを示す情報を返却して（ステップS307）、発行済みチケットチェック処理を終了し、図8のチケット購入処理に復帰する。

【0101】

図8のチケット購入処理に復帰すると、CPU11は、発行済みチケットチェック処理において未発行が返却されたかどうかを判定する（ステップS256）。発行済みが返却されていた場合には、ステップS254の処理に戻り、別のパターンを有する二次元バーコードからなるチケット100を生成する。

【0102】

発行済みが返却されていた場合には、CPU11は、共に返却された暗号化値a'に対応する第1テーブル143の記憶位置と、暗号化値b'に対応する第2テーブル144の記憶位置とに、購入要求と共に受信したユーザIDとチケットNo.とを組にして登録する（ステップS257）。CPU11は、さらに当該購入要求に含まれるユーザID及びチケットNo.に対応するユーザデータベース142のフラグを予約済みを示す1から購入済みを示す2に更新する（ステップS258）。

【0103】

フラグの更新が終了すると、CPU11は、購入要求をした携帯電話機3に宛てたメールで、通信装置13から発行したチケットの二次元バーコードの画像データを送信させる（ステップS259）。チケットの画像データを携帯電話機3に送信した後、CPU11は、当該チケットの画像データをサーバ装置1内に残さないように破棄する（ステップS260）。チケットを送信し、これを破棄することにより、サーバ装置1の側における処理は終了となる。

【0104】

また、購入要求に含まれるユーザIDが登録されていないかパスワードが間違っていた場合、或いは購入要求に含まれるユーザID及びチケットNo.に対応するフラグが予約済みを示していなかった場合には、CPU11は、購入要求をした携帯電話機3に宛てたメールで、通信装置13から購入不可通知を送信させる（ステップS261）。購入不可通知の送信により、サーバ装置1の側における処理は終了となる。

【0105】

携帯電話機3では、通信装置36がステップS259で送信されたチケットまたはステッ

10

20

30

40

50

プ S 2 6 1 で送信された購入不可通知を受信する（ステップ S 2 0 3）。CPU 3 1 は、受信したチケットまたは購入不可通知を表示装置 3 5 に表示させて、ユーザに示す（ステップ S 2 0 4）。これで、チケット購入処理が終了する。なお、ここで受信したチケットは、ユーザが入力装置 3 4 から所定の操作を行うことで、いつでも表示装置 3 5 に表示させることができる。

【 0 1 0 6 】

図 1 0 は、チケットキャンセル処理を示すフローチャートである。チケットキャンセル処理においても、ユーザは、自己の携帯電話機 3 の入力装置 3 4 から、ユーザ ID とパスワードとを入力する。また、購入したチケットのうちからキャンセルしようとするチケットのチケット No. を入力装置 3 4 から入力する（ステップ S 4 0 1）。さらにユーザが入力装置 3 4 からキャンセルの要求を入力すると、ステップ S 4 0 1 で入力されたユーザ ID、パスワード及びチケット No. と共にキャンセル要求が通信装置 3 6 からサーバ装置 1 に送信される（ステップ S 4 0 2）。その後、CPU 3 1 は、サーバ装置 1 からの情報の受信待ちとなる。

10

【 0 1 0 7 】

サーバ装置 1 では、通信装置 1 3 が携帯電話機 3 から送られてきたキャンセル要求を受信する（ステップ S 4 5 1）。このキャンセル要求を受信すると、CPU 1 1 は、受信したキャンセル要求に含まれるユーザ ID がユーザデータベース 1 4 2 に登録されているかどうかを判定する。さらに、パスワードが正しいかどうかを判定する（ステップ S 4 5 2）。

20

【 0 1 0 8 】

ユーザ ID が登録されていて、パスワードも正しい場合には、CPU 1 1 は、受信したキャンセル要求に含まれるユーザ ID 及びチケット No. に対応するユーザデータベース 1 4 2 のフラグの状態がチケットの購入済みを示す 2 になっているかどうかを判定する（ステップ S 4 5 3）。

【 0 1 0 9 】

フラグの状態が購入済みを示す 2 になっていれば、CPU 1 1 は、キャンセル要求に含まれるユーザ ID 及びチケット No. の組を第 1 テーブル 1 4 3 及び第 2 テーブル 1 4 4 からサーチする（ステップ S 4 5 4）。そして、サーチされたユーザ ID 及びチケット No. の組を第 1 テーブル 1 4 3 及び第 2 テーブル 1 4 4 から削除する（ステップ S 4 5 5）。これにより、キャンセルしたチケットは使用不能となる。また、CPU 1 1 は、当該キャンセル要求に含まれるユーザ ID 及びチケット No. に対応するユーザデータベース 1 4 2 のフラグを購入済みを示す 2 から未予約を示す 0 に更新する（ステップ S 4 5 6）。

30

【 0 1 1 0 】

フラグの更新が終了すると、CPU 1 1 は、キャンセル要求をした携帯電話機 3 に宛てたメールで、通信装置 1 3 からキャンセル完了通知を送信させる（ステップ S 4 5 7）。また、キャンセル要求に含まれるユーザ ID が登録されていないかパスワードが間違っていた場合、或いはキャンセル要求に含まれるユーザ ID 及びチケット No. に対応するフラグが購入済みを示していなかった場合には、CPU 1 1 は、キャンセル要求をした携帯電話機 3 に宛てたメールで、通信装置 1 3 からチケットなし通知を送信させる（ステップ S 4 5 8）。キャンセル完了通知またはチケットなし通知の送信により、サーバ装置 1 の側における処理は終了となる。

40

【 0 1 1 1 】

携帯電話機 3 では、通信装置 3 6 がステップ S 4 5 7 で送信されたキャンセル完了通知またはステップ S 4 5 8 で送信されたチケットなし通知を受信する（ステップ S 4 0 3）。CPU 3 1 は、受信したキャンセル完了通知またはチケットなし通知を表示装置 3 5 に表示させて、ユーザに示す（ステップ S 4 0 4）。これで、チケットキャンセル処理が終了する。

【 0 1 1 2 】

図 1 1 は、チケット再発行処理を示すフローチャートである。チケットを紛失するなどし

50

て再発行を受けようとするユーザは、自己の携帯電話機3の入力装置34から、ユーザIDとパスワードとを入力する。また、再発行を受けようとするチケットのチケットNo.を入力装置34から入力する(ステップS501)。さらにユーザが入力装置から再発行の要求を入力すると、ステップS501で入力されたユーザID、パスワード及びチケットNo.と共に再発行要求が通信装置36からサーバ装置1に送信される(ステップS502)。その後、CPU31は、サーバ装置1からの情報の受信待ちとなる。

【0113】

サーバ装置1では、通信装置13が携帯電話機3から送られてきた再発行要求を受信する(ステップS551)。この再発行要求を受信すると、CPU11は、受信した再発行要求に含まれるユーザIDがユーザデータベース142に登録されているかどうかを判定する。さらに、パスワードが正しいかどうかを判定する(ステップS552)。

10

【0114】

ユーザIDが登録されていて、パスワードも正しい場合には、CPU11は、受信した再発行要求に含まれるユーザID及びチケットNo.に対応するユーザデータベース142のフラグの状態がチケットの購入済みを示す2になっているかどうかを判定する(ステップS553)。

【0115】

フラグの状態が購入済みを示す2になっていれば、CPU11は、再発行要求に含まれるユーザID及びチケットNo.の組を第1テーブル143及び第2テーブル144からサーチする(ステップS554)。そして、サーチされたユーザID及びチケットNo.の組を第1テーブル143及び第2テーブル144から削除する(ステップS555)。これにより、既に発行されていた再発行前のチケットは使用不能となる。

20

【0116】

既に発行されていたチケットを使用不能とした後、CPU11は、ランダムにパターンを決定して二次元バーコードからなるチケット100を新たに生成する(ステップS556)。CPU11は、生成したチケットが既に発行済みのチケット(使用不能とされたものを含まない)のパターンと同じであるかどうかをチェックする発行済みチェック処理を行う(ステップS557)。発行済みチケットチェック処理は、ステップS255のものと同一である。

【0117】

発行済みチケットチェック処理を終了し、チケット再発行処理に復帰すると、CPU11は、発行済みチケットチェック処理において未発行が返却されたかどうかを判定する(ステップS558)。発行済みが返却されていた場合には、ステップS556の処理に戻り、別のパターンを有する二次元バーコードからなるチケット100を生成する。

30

【0118】

発行済みが返却されていた場合には、CPU11は、共に返却された暗号化値a'に対応する第1テーブル143の記憶位置と、暗号化値b'に対応する第2テーブル144の記憶位置とに、購入要求と共に受信したユーザIDとチケットNo.とを組にして登録する(ステップS559)。ユーザがチケットを購入している状態には変わらないので、ここのフラグ更新は行われない。

40

【0119】

第1テーブル143及び第2テーブルへの登録が終了すると、CPU11は、再発行要求をした携帯電話機3に宛てたメールで、通信装置13から再発行したチケットの二次元バーコードの画像データを送信させる(ステップS560)。チケットの画像データを携帯電話機3に送信した後、CPU11は、当該チケットの画像データをサーバ装置1内に残さないように破棄する(ステップS561)。再発行したチケットを送信し、これを破棄することにより、サーバ装置1の側における処理は終了となる。

【0120】

また、再発行要求に含まれるユーザIDが登録されていないかパスワードが間違っていた場合、或いは再発行要求に含まれるユーザID及びチケットNo.に対応するフラグが購

50

入済みを示していなかった場合には、CPU 11は、再発行要求をした携帯電話機3に宛てたメールで、通信装置13からチケットなし通知を送信させる（ステップS562）。チケットなし通知の送信により、サーバ装置1の側における処理は終了となる。

【0121】

携帯電話機3では、通信装置36がステップS560で送信されたチケットまたはステップS572で送信されたチケットなし通知を受信する（ステップS503）。CPU31は、受信したチケットまたはチケットなし通知を表示装置35に表示させて、ユーザに示す（ステップS504）。これで、チケット再発行処理が終了する。ここで受信したチケットも、ユーザが入力装置34から所定の操作を行うことで、いつでも表示装置35に表示させることができる。

10

【0122】

図12は、チケット認証処理を示すフローチャートである。チケットを購入したユーザが、イベント会場に入場しようとする場合、当該イベントに対応したチケットを自分の携帯電話機3の表示装置35に表示させる。そして、二次元バーコードからなるチケットが表示された表示装置35を、入場ゲート装置2のバーコードリーダ24に押し当てる。

【0123】

入場ゲート装置2では、バーコードリーダ24が携帯電話機3の表示装置35に表示されたチケットを読み取り、これをCPU21に渡す（ステップS601）。CPU21は、発行時または再発行時にサーバ装置1が行ったのと同じ方法により、読み取ったチケットのパターンに対応した数値Xを生成する。チケットの向きは、方向チェックマーク101～104により分かる（ステップS602）。さらに、CPU21は、発行時または再発行時にサーバ装置1が行ったのと同様に、チケットを数値化した数値Xを除数Aで除算して剰余aを求め、また、数値Xを除数Bで除算して剰余bを求める（ステップS603）。

20

【0124】

CPU21は、さらに、発行時または再発行時にサーバ装置1が行ったのと同様に、求めた剰余aを所定の暗号鍵を用いて暗号化して暗号化値a'を生成し、また、剰余bも同様に暗号化して暗号化値b'を生成する（ステップS604）。CPU21は、生成した暗号化値a'、b'を、通信装置23からサーバ装置1に送信させる（ステップS605）。

30

【0125】

サーバ装置1では、通信装置13が入場ゲート装置2から送られてきた暗号化値a'、b'を受信する（ステップS651）。暗号化値a'、b'を受信すると、CPU11は、受信した暗号化値a'、b'に従ってテーブルチェック処理を行う（ステップS652）。テーブルチェック処理は、ステップS304のものと同一である。

【0126】

テーブルチェック処理を終了し、チケット認証処理に復帰すると、CPU11は、テーブルチェック処理から返却された情報が一致を示す情報か不一致を示す情報であるかを判定する（ステップS653）。一致を示す情報であったならば、テーブルチェック処理において第1テーブル143及び第2テーブル144からユーザIDとの組で取り出したチケットNo.が、当該イベントを示すものであるかどうかを判定する（ステップS654）。

40

【0127】

取り出したチケットNo.が当該イベントを示すものであった場合には、CPU11は、通信装置13から開放許可通知を入場ゲート装置2に送信させる（ステップS655）。CPU11は、さらにテーブルチェック処理において第1テーブル143及び第2テーブル144から取り出したユーザID及びチケットNo.に対応するユーザデータベース142のフラグを購入済みを示す2から使用済みを示す3に更新する（ステップS656）。

【0128】

50

また、第1テーブル143及び第2テーブル144から取り出したユーザID及びチケットNo.の組が一致していなかった場合、或いはチケットNo.が当該イベントを示すものでなかった場合には、CPU11は、通信装置13からアラーム通知を入場ゲート装置2に送信させる(ステップS657)。アラーム通知は、第1テーブル143及び第2テーブル144から取り出したユーザID及びチケットNo.の組が一致していなかった場合と、チケットNo.が当該イベントを示すものでなかった場合とで内容の異なるものとしてもよい。フラグの更新またはアラーム通知の送信により、サーバ装置1の側における処理は終了となる。

【0129】

入場ゲート装置2では、通信装置23がステップS655で送信された開放通知またはステップS657で送信されたアラーム通知を受信する(ステップS606)。CPU21は、受信したのが開放通知であるかアラーム通知であるかを判定する(ステップS607)。開放通知であれば、CPU21は、入場ゲート25を開放状態とさせて、ユーザがイベント会場に入場できるようにする(ステップS608)。アラーム通知であれば、CPU21は、アラーム装置26を発報させる(ステップS609)。入場ゲート25の開放またはアラームの発報により、チケット認証処理が終了する。

【0130】

以上説明したように、この実施の形態にかかるチケット発行システムでは、ユーザが購入したイベントのチケットを携帯電話機3に送信するに当たって、サーバ装置1は、そのチケットに対応した数値Xに基づいて暗号化値a'、b'を生成し、第1テーブル143の暗号化値a'に対応する記憶位置と第2テーブル144の暗号化値b'に対応する記憶位置とに、ユーザIDとチケットNo.の組を登録している。そして、チケットをユーザの携帯電話機3に送信している。

【0131】

一方、入場ゲート装置2では、ユーザの携帯電話機3の表示装置35に表示されたチケットを読み取り、読み取ったチケットを数値化し、暗号化値a'、b'を求めて、サーバ装置1に送信している。サーバ装置1では、受信した暗号化値a'、b'に従って第1テーブル143及び第2テーブル144を参照して、チケットが正当なものであるかどうかを認証している。すなわち、二次元バーコードからなるチケットのパターンを照合することなく、第1テーブル143と第2テーブル144を参照するだけで、チケットの認証を高速に行うことができる。

【0132】

チケットのパターンに対応した数値Xを除算する除数A、Bの最小公倍数は、数値Xがとりうる最大値Xmaxと最小値Xminの差より大きいという関係がある。この関係を満たす限り、異なるパターンのチケットでは、剰余a、bの両方が一致することがなく、これらを暗号化した暗号化値a'、b'の両方が一致することもない。第1テーブル143の暗号化値a'に対応する記憶位置と第2テーブル144の暗号化値b'に対応する記憶位置とに、同じユーザID及びチケットNo.の組が登録されるチケットのパターンは、1つだけということとなる。従って、個々のチケットのパターンからユーザ及びチケットNo.を一義的に特定することができる。

【0133】

このように第1テーブル143及び第2テーブル144を参照するだけで、個々のチケットのパターンからユーザ及びチケットNo.を一義的に特定することができるので、発行した各チケットの二次元バーコードのパターンをサーバ装置1に残しておく必要がない。二次元バーコードのパターンは、情報量が大きくなるものなので、これを残さないでよいことから、サーバ装置1の記憶容量が小さくても済むことになる。

【0134】

また、チケットのパターンは、サーバ装置1に残さないでよいことから、サーバ装置1をハッキングしても盗み出されることがないので、セキュリティが高いものとなる。ハッキングに備えて暗号化して保存するのとは異なり、チケットの発行時においてチケットのパタ

10

20

30

40

50

ーンを暗号化したり、チケットの認証時においてチケットのパターンを復号化するという処理は必要ない。このため、高度のセキュリティを達成しつつ、サーバ装置 1 の処理量を小さくすることができる。

【0135】

もつとも、剰余 a、b と、除数 A、B と、チケットのパターンから数値 X を生成する方法が分かっしまえば、チケットのパターンを復元できてしまう。ところが、第 1 テーブル 143 及び第 2 テーブル 144 にユーザ ID 及びチケット No. の組を登録する記憶位置は、剰余 a、b に対応する記憶位置ではなく、暗号化値 a'、b' に対応した記憶位置としている。

【0136】

ユーザ ID 及びチケット No. の組の記憶位置から暗号化値 a'、b' の値は分かっしまいが、暗号化値 a'、b' を復号化する処理は一切行う必要がないので、これを復号化する復号鍵は、サーバ装置 1 にも入場ゲート装置 2 にも置いていない。このため、サーバ装置 1 及び入場ゲート装置 2 がハッキングされても、剰余 a、b の値を知ることができないので、ここから不正に読み出された情報のみに基づいてチケットのパターンを復元することはできない。

【0137】

仮にチケットのパターンを復元しようとするのであれば、オブジェクトコードで記述されたプログラムを解析して除数 A、B を抜き出し、チケットのパターンから数値 X を生成する方法を解読し、さらに第 1 テーブル 143 及び第 2 テーブル 144 に対応したアドレスと暗号化値 a'、b' との関係を解読しなければならない。その上で、暗号化値 a'、b' を剰余 a、b に復号化する復号鍵を見つけ出さなければならない。このため、剰余 a、b の暗号化強度がそれほど高くなくても、全体としては、最強と呼ばれるような暗号アルゴリズムに比べても遜色がない、或いはそれ以上のセキュリティを達成することができるようになる。

【0138】

また、第 1 テーブル 143 及び第 2 テーブル 144 には、ユーザ ID だけでなく、チケット No. も組み合わせて登録している。第 1 テーブル 143 及び第 2 テーブル 144 から取り出したユーザ ID とチケット No. の両方が一致していなければ、イベント会場への入場はできない。このため、1 人のユーザが異なるイベントについて複数のチケットを購入して使えるようにしても、各イベントに対してチケットを購入したユーザだけが、当該イベントの会場に入場できるようにすることができる。

【0139】

さらに、1 人のユーザが複数のチケットを購入して使えるようにすることで、チケットとして発行される二次元バーコードの数がユーザ数よりも大幅に増えることとなる。しかし、ユーザの携帯電話機 3 に送信した後は二次元バーコードからなるチケットを保存せず、また、二次元バーコード同士を照合することも一切行っていない。このため、チケットの数の増加による処理量や記憶容量の増加は、チケットの数の増加に比べると無視できる程度に僅かなものとすることができる。

【0140】

この実施の形態にかかるチケット発行システムでは、上記したように必要となる処理量や記憶容量が大きく増えることはないので、複雑なパターンの二次元バーコードをチケットに適用することができる。複雑なパターンの二次元バーコードを使用することで、適当に生成したパターンが各イベントについて発行したチケットのパターンと一致する確率は、数万～数百万分の 1 以下という極めて小さな値とすることもできる。

【0141】

また、発行済みのチケットに適用された二次元バーコードのパターンは、サーバ装置 1 にも入場ゲート装置 2 にも残っておらず、チケットを購入したユーザの携帯電話機 3 においてのみ管理されるだけである。このため、偽造のチケットによりイベント会場に不正な入場があった場合、その責任はユーザ側にある場合がほとんどである。従って、システムの

10

20

30

40

50

提供者がイベントの開催者から、不正な入場に対する責任を問われる場合がほとんどなくて済むようになる。

【0142】

ところで、上記のチケット発行システムにおける処理は、チケット予約処理、チケット購入処理、チケットキャンセル処理、チケット再発行処理、及びチケット認証処理の5つに大きく分けられるが、このうちで短時間のうちに処理が集中すると考えられるのは、チケット予約処理とチケット認証処理の2つだけである。チケット購入処理、チケットキャンセル処理、チケット再発行処理は、チケットの予約を行った後、イベントの開始までの任意の時に行われるものだからである。

【0143】

チケットに適用される二次元バーコードのパターンの生成や、数値化、剰余の算出、暗号化値の生成といった比較的処理量が多い（もっとも、バーコードの照合に比べれば小さいが）処理は、処理の集中する時間においてサーバ装置1が実行する必要がない。チケット認証処理においては、処理が集中する時間に入場ゲート装置2が読み取ったチケットの数値化、剰余の算出、暗号化値の生成といった比較的処理量が多い処理を行わなければならないが、入場ゲート装置2は実際には複数あって、それぞれに処理を分散できる。

【0144】

このため、チケット予約処理及びチケット認証処理に対応するため、必要以上に処理能力が高いサーバ装置1を用意しておく必要がない。また、比較的処理量が多い処理は分散して行われるため、サーバ装置1を無駄なく稼働させることができるようになる。

【0145】

本発明は、上記の実施の形態に限られず、種々の変形、応用が可能である。以下、本発明に適用可能な上記の実施の形態の変形態様について説明する。

【0146】

上記の実施の形態では、サーバ装置1は、ユーザIDとパスワードとを用いて、ユーザデータベース142に登録されたユーザを認証し、特定するものとしていた。これに対して、サーバ装置1が自動音声応答によりチケットの購入予約や販売等の処理を行うものとする場合、携帯電話機3からの着呼時に通知される発信者番号を用いて、ユーザデータベース142に登録されたユーザを認証し、特定するものとしてもよい。

【0147】

上記の実施の形態では、チケットに対応した数値を、そのまま除数A、Bで除算して、剰余a、bを求めるものとしていた。これに対して、チケットに対応した数値から該数値がとり得る最小値を減算した値、またはチケットに対応した数値がとり得る値の最大値からチケットに対応する数値を減算した値を、数値A、Bで除算して、剰余a、bを求めるものとしてもよい。この場合、チケットに対応した数値がとり得る値の範囲によっては、被除数がかなり小さくなって、除算の処理が高速化される。

【0148】

上記の実施の形態では、チケットの認証を行うために、第1テーブル143と第2テーブル144の2つのテーブルを用いていた。これに対して、3つ以上のテーブルを用いてチケットの認証を行うものとしてもよい。チケットに対応した数値は、それぞれのテーブル毎に異なる除数で除算して剰余を求めるものとしてすることができる。3つ以上の除数の最小公倍数が、チケットに対応した数値の最大値と最小値との差より大きくなればよい。さらにそれぞれの剰余を暗号化した暗号化値に従って、各テーブルを参照するものとするればよい。3つ以上のテーブルを用いた場合には、全てのテーブルでユーザIDとチケットNo.の組が一致するかどうかを調べるものとするればよい。

【0149】

上記の実施の形態では、チケットに対応した数値を除数A、Bで除算した剰余を求め、さらにこれを暗号化した暗号化値a'、b'を生成していた。この暗号化値a'、b'の組み合わせは、チケットのパターン毎に異なるものとなっていた。しかしながら、チケットに対応した数値から求められる複数の数値の組がチケットのパターン毎に異なるものとな

10

20

30

40

50

るのであれば、上記とは別の演算式を適用することができる。さらに、チケットを複数の領域に分割し、各領域をそのまま数値化した複数の数値の組は、チケットのパターン毎に異なるものとなるので、上記したような演算で求められる数値の組に代えて適用することもできる。

【0150】

上記の実施の形態では、チケットに対応した数値を除算した後の剰余だけを暗号化するものとしていた。これに対して、サーバ装置1及び入場ゲート装置2では、チケットのパターンを数値化した後に暗号化し、暗号化した数値を除算して剰余を求めるものとしてもよい。この剰余をさらに暗号化するものとしてもよい。ここで、チケットに対応した数値を暗号化する暗号鍵にも、復号鍵が異なる非対称暗号系の暗号鍵を適用することができる。ここでも、暗号化した数値の復号化を一切行う必要がないからである。この場合には、サーバ装置1から情報が盗み出されても、盗み出した情報からチケットを復元することはさらに困難となるので、よりセキュリティの高いシステムを構成することができる。

10

【0151】

上記の実施の形態では、サーバ装置1は、チケットを販売または再発行する際に、二次元バーコードによるパターンを生成してから、これを数値化するものとしていた。これに対して、ランダムに生成した数値から暗号化値 a' 、 b' までを求め、第1テーブル143及び第2テーブル144を参照した結果として発行済みでないことが分かってから、数値に対応したパターンを生成して二次元バーコードのチケットとして携帯電話機3に宛てて送信するものとしてもよい。この場合、実際には使用できないチケットはパターンまでを生成する必要がなくなるので、余分な処理が行わないで済むようになる。

20

【0152】

上記の実施の形態では、チケットとして用いられる二次元バーコードのパターンは、サーバ装置1から携帯電話機3に送られると、すぐに表示装置35に表示できるものとしていた。しかし、この場合には、表示装置35に表示されたパターンを見た者が同じ画像を生成して、チケットを偽造することができるようになってしまう。そこで、所定の暗証番号を入力しなければ、送信した二次元バーコードのパターンを表示装置35に表示できないようにしてもよい。入場ゲート装置2の直前で暗証番号を提示すれば、正規に販売したチケットと同じパターンを予め生成しておくことが実施的に不可能となり、不正なチケットによるイベント会場への不正入場を防ぐことができるようになる。

30

【0153】

上記の実施の形態では、ユーザが購入したチケットまたは再発行を受けたチケットは、携帯電話機3にメールで送信されるものとしていた。しかしながら、ユーザがメールの転送設定を行っていれば、本当はチケットを購入していない者にもチケットを含むメールが送られてしまうこととなる。これに対して、携帯電話会社の公式サイトとしてチケットの販売等を行えば、サーバ装置1が携帯電話機3から購入要求や再発行要求を受信したときに、ユーザの携帯電話機3の個体番号が通知されてきている。

【0154】

そこで、サーバ装置1は、通知された個体番号を暗号鍵として用いてチケットを暗号化して送信し、携帯電話機3において個体番号を復号鍵として用いて復号するようにしてもよい。これにより、本当はチケットを購入していない者にチケットを含むメールが転送されても、その二次元バーコードのパターンを正しく復号して表示できなくなる。これにより、サーバ装置1から携帯電話機3への送信途中で盗み出されたチケットや、不正に転送されたチケットによるイベント会場への不正入場を防ぐことができるようになる。

40

【0155】

上記の実施の形態では、チケットは、二階調の二次元バーコードによって構成され、携帯電話機3の表示装置35に表示されるものとしていた。これに対して、多階調のパターンを有するバーコードや、三次元のパターンを有するバーコードをチケットに適用することもできる。この三次元バーコードは、例えばポリゴンで形成された立方体の各面に二次元のバーコードを表示させたものであり、Java（登録商標）等のアプリケーションによ

50

ってポリゴンが回転される。入場ゲート装置2のCPU21は、ポリゴンの回転によって立方体の各面に表示されたコードを全て認識することができる。三次元バーコードは、二次元バーコードより情報量を大きくすることができるが、三次元バーコードのように情報量が大きい識別情報では、必要な記憶容量を小さくできるという効果が顕著に現れる。

【0156】

入場ゲート装置2と携帯電話機3とをブルートゥース技術の適用などにより直接通信可能に構成した場合には、チケットして視認不可能な情報であっても、上記した二次元バーコードの代わりに適用することができる。どのような形態の識別情報であっても、それを数値化した後に上記の実施の形態と同様に暗号化値a'、b'までを求め、この暗号化値a'、b'を用いて、第1テーブル143及び第2テーブル144を参照するという構成を採用することができる。

10

【0157】

上記の実施の形態では、イベントのチケットを二次元バーコードによって構成した場合に、その認証のための技術として本発明を適用した場合について説明した。しかしながら、本発明の適用範囲はイベントのチケットに限るものではなく、1人のユーザが複数の識別情報を使い分けて認証を受ける場合全般に適用することができる。

【0158】

上記の実施の形態では、サーバ装置1、入場ゲート装置2、及び携帯電話機3の処理プログラムは、それぞれ主記憶装置12、記憶装置22、或いはROM32に予め記憶されているものとして説明した。これに対して、これらの処理プログラムの全部または一部のみをCD-ROMやDVD-ROMなどのコンピュータ読み取り可能な記録媒体に格納して、ハードウェアとは別に配布するものとしてもよい。また、これらの処理プログラムの全部または一部をインターネット上のWebサーバ装置が有する固定ディスク装置に格納しておき、サーバ装置1、入場ゲート装置2、或いは携帯電話機3からの要求に従って、インターネットなどのネットワークを通じて配信するものとしてもよい。

20

【0159】

【発明の効果】

以上説明したように、本発明によれば、識別情報の発行及び認証において、認証処理の高速化とセキュリティの向上とを同時に達成することができる。

【0160】

また、識別情報の発行及び認証において、例えば1人のユーザが複数の識別情報を使い分けることなどにより、発行される識別情報の数が増えても、処理量をあまり増大させることがない。

30

【図面の簡単な説明】

【図1】本発明の実施の形態にかかるチケット発行システムを示すブロック図である。

【図2】図1のサーバ装置の構成を示すブロック図である。

【図3】二次元バーコードにより構成されるチケットの例を示す図である。

【図4】図2のユーザデータベースと、第1、第2のテーブルを示す図である。

【図5】図1の携帯電話機の構成を示すブロック図である。

【図6】図1の入場ゲート装置の構成を示すブロック図である。

40

【図7】チケット予約処理を示すフローチャートである。

【図8】チケット購入処理を示すフローチャートである。

【図9】図8の発行済みチケットチェック処理を詳細に示すフローチャートである。

【図10】チケットキャンセル処理を示すフローチャートである。

【図11】チケット再発行処理を示すフローチャートである。

【図12】チケット認証処理を示すフローチャートである。

【符号の説明】

- 1 サーバ装置
- 2 入場ゲート装置
- 3 携帯電話機

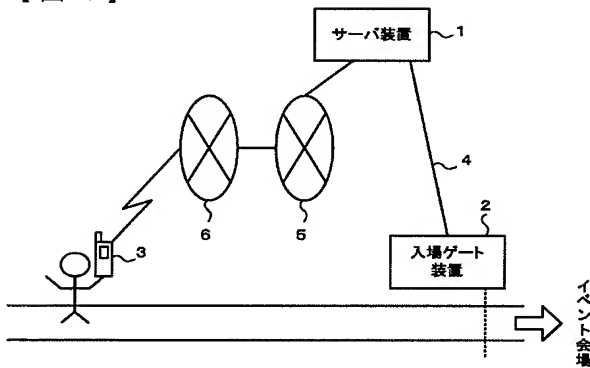
50

- 4 専用線
- 5 インターネット
- 6 携帯電話網
- 11 CPU
- 12 主記憶装置
- 13 通信装置
- 14 補助記憶装置
- 21 CPU
- 22 記憶装置
- 23 通信装置
- 24 バーコードリーダー
- 25 入場ゲート
- 31 CPU
- 32 ROM
- 33 RAM
- 34 入力装置
- 35 表示装置
- 36 通信装置
- 100 チケット（二次元バーコード）
- 101～104 方向チェックマーク
- 105 チケット表示部
- 141 プログラムファイル
- 142 ユーザデータベース
- 143 第1テーブル
- 144 第2テーブル

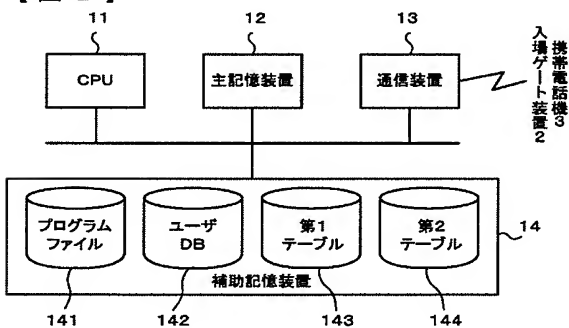
10

20

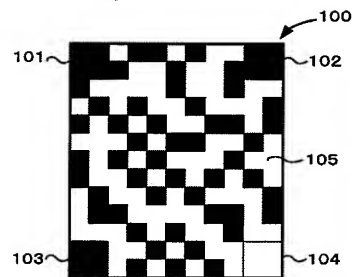
【図1】



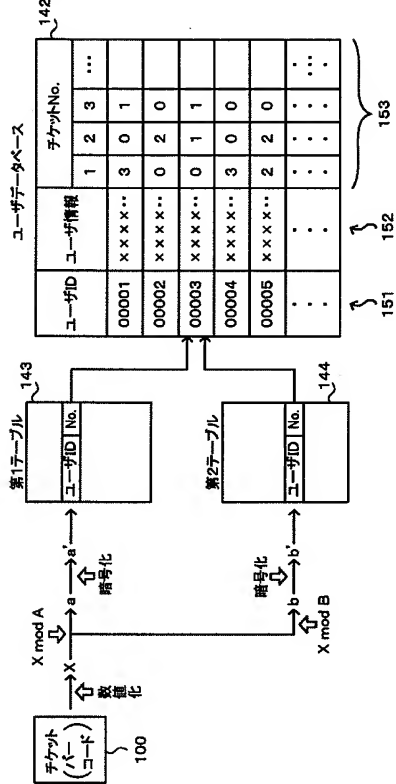
【図2】



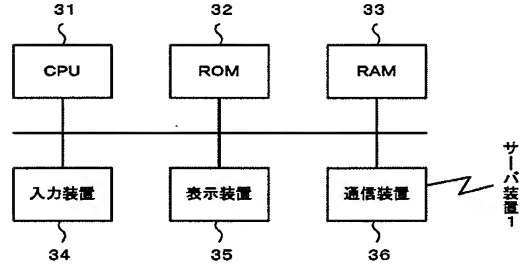
【図3】



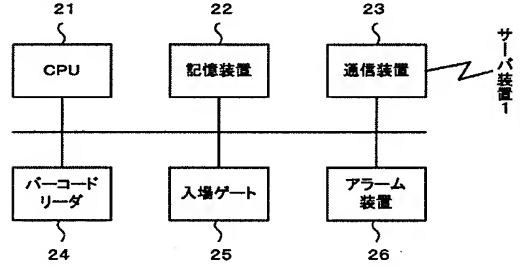
【図 4】



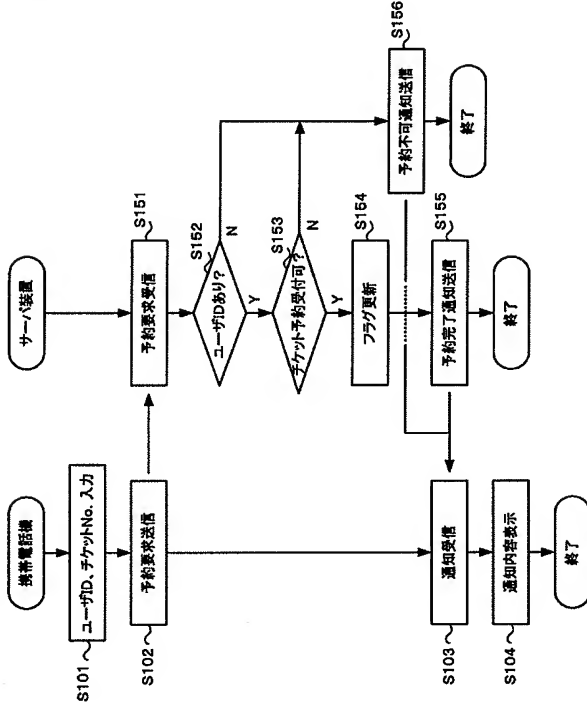
【図 5】



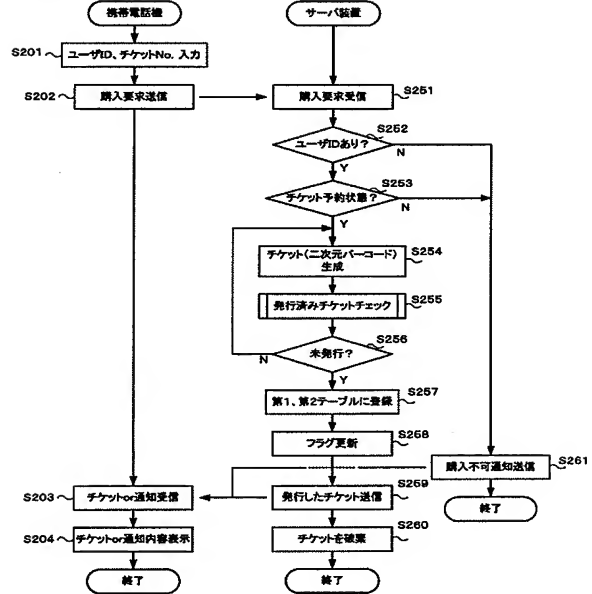
【図 6】



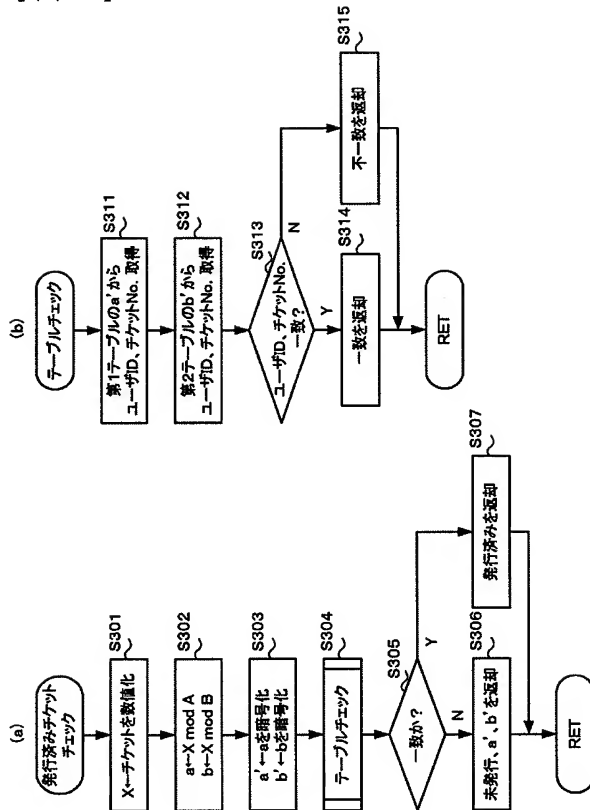
【図 7】



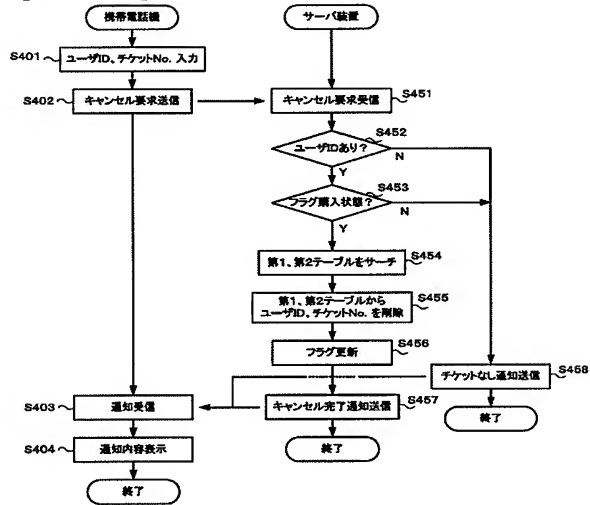
【図 8】



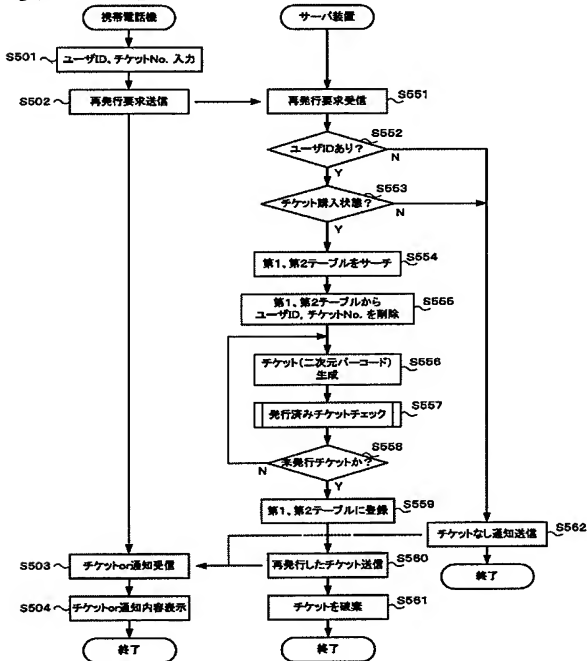
【図 9】



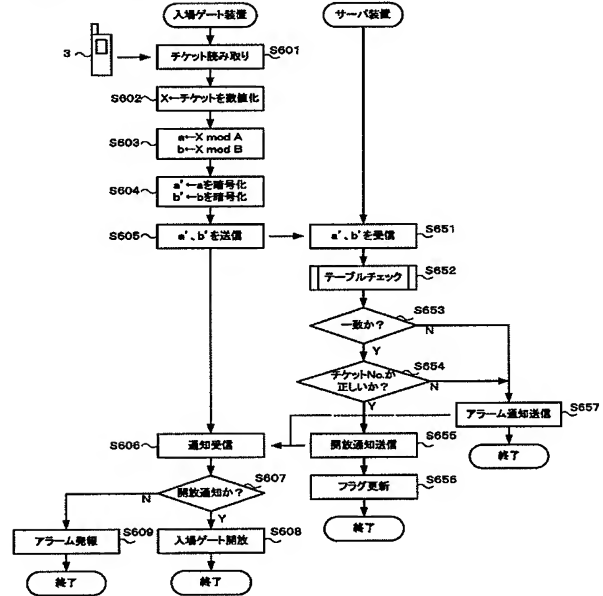
【図 10】



【図 11】



【図 12】



フロントページの続き

(51) Int. Cl. ⁷	F I	テーマコード (参考)
G 0 6 K 17/00	G 0 6 K 7/10	Z 5 J 1 0 4
G 0 6 K 19/07	G 0 6 K 17/00	T
G 0 9 C 1/00	G 0 9 C 1/00	6 5 0 Z
H 0 4 L 9/32	H 0 4 L 9/00	6 7 5 B
	G 0 6 K 19/00	Z E C J

F ターム(参考) 5B082 EA11

5B085 AA08 AE09 AE15 AE23 AE29 BE04 BG02 CA02 CA04 CA07

5J104 AA12 KA05 NA02 NA18